Chapter 1

IT Governance and Management

THE CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) OBJECTIVES REPRESENT 18% OF THE MATERIAL COVERED ON THE EXAM AND INCLUDE:

✓ **Domain 2: Governance & Management of IT**

A. IT Governance

1. IT Governance and IT Strategy
2. IT-Related Frameworks
3. IT Standards, Policies, and Procedures
4. Organizational Structure
5. Enterprise Architecture
6. Enterprise Risk Management
7. Maturity Models
8. Organization

B. IT Management

1. IT Resource Management
2. IT Service Provider Acquisition and Management
3. IT Performance Monitoring and Reporting
4. Quality Assurance and Quality Management of IT

Supporting Tasks

5. Evaluate the IT strategy for alignment with the organization's strategies and objectives.
6. Evaluate the effectiveness of IT governance structure and IT organizational structure.
7. Evaluate the organization's management of IT policies and practices.

8. Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements.

10. Evaluate the organization's risk management policies and practices.

15. Evaluate whether IT supplier selection and contract management processes align with business requirements.

22. Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives.

37. Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.

IT governance should be the wellspring from which all other IT activities flow.

Properly implemented, governance is a process whereby senior management exerts strategic control over business functions through policies, objectives, delegation of authority, and monitoring. Governance is management's control over all other IT processes to ensure that IT processes continue to meet the organization's business objectives effectively.

Business alignment is a critical characteristic of IT governance. IT's primary mission should be the support of the overall business mission, goals, and objectives. The alignment of IT to the business must be intentional and deliberate for IT and the organization to succeed.

Organizations usually establish governance through an IT steering committee that is responsible for setting long-term IT strategy and by making changes to ensure that IT processes continue to support IT strategy and the organization's needs. This is accomplished through the development and enforcement of IT policies, requirements, and standards.

IT governance typically focuses on several key processes, such as personnel management, sourcing, change management, financial management, quality management, security management, and performance optimization. Another key component is the establishment of an effective organization structure and clear statements of roles and responsibilities. An effective governance program will use a balanced scorecard (BSC) or other means to monitor these and other key processes, and through a process of continuous improvement, IT processes will be changed to remain effective, to support ongoing business needs, and to respond to existing and emerging risks.

IT Governance Practices for Executives and Boards of Directors

Governance starts at the top, and a proper "tone at the top" is crucial for effective governance and oversight.

Whether the organization has a board of directors, council members, commissioners, or some other top-level governing body, governance begins with the establishment of top-level objectives and policies that are translated into more actions, policies, processes, procedures, and other activities downward through each level in the organization.

This section describes governance practices recommended for IT organizations, including a strategy-developing committee, measurement via the BSC, and security management.

Governance is not merely an IT practice. Rather, governance is practiced in the business apart from IT to facilitate management's control over all aspects of business operations, including IT.

IT Governance

The purpose of IT governance is to align IT with the strategies and objectives of the organization. The term IT governance refers to a collection of top-down activities intended to control the IT organization from a strategic perspective to ensure that the IT organization supports the business. The artifacts and activities that flow out of healthy IT governance include the following:

- **Policy:** At a minimum, IT policy should directly reflect the mission, objectives, and goals of the overall organization.
- **Priorities:** Priorities in the IT organization should flow directly from the organization's mission, objectives, and goals. Whatever is most important to the organization as a whole should be important to IT as well.
- **Standards:** The technologies, protocols, and practices used by IT should reflect the organization's needs. On their own, standards help to drive a consistent approach to solving business challenges; the choice of standards should facilitate solutions that meet the organization's needs in a cost-effective and secure manner.
- **Resource management:** The budget, personnel, equipment, and other resources are planned, selected, managed, and measured to ensure that the IT organization has the ability to meet its objectives.
- **Vendor management:** The suppliers and service providers that IT selects should reflect IT and business priorities, standards, and practices.
- **Program and project management:** IT programs and projects should be organized and performed in a consistent manner that reflects IT and business priorities and supports the business.

While IT governance contains the elements just described, strategic planning is also a key component of governance. Strategy development is discussed in the next section.

IT Governance Frameworks

Every organization may have a unique mission, objectives, goals, business models, tolerance for risk, and so on, but organizations need not invent governance frameworks from scratch

to manage their IT and business objectives. Several good frameworks can be adapted to meet organizations' needs, including the following:

- **COBIT 2019:** This IT management framework was developed by the IT Governance Institute and ISACA. COBIT's five domains are:
  - Evaluate, Direct, and Monitor
  - Align, Plan, and Organize
  - Build, Acquire, and Implement
  - Deliver, Service, and Support
  - Monitor, Evaluate, and Assess
- **ISO/IEC 27001:** This is the well-known international standard for top-down information security management. In the context of IT security governance, most important here are the requirements in ISO/IEC 27001, not the security controls that appear in its appendix. This is a good opportunity to point out that governance frameworks and control frameworks are not the same thing.
- **ITIL:** Formerly an acronym for IT Infrastructure Library, ITIL is a framework of processes for IT service delivery. ITIL was originally sponsored by the UK Office of Government Commerce to improve its IT management processes, but it is now owned by an organization named AXELOS. The international standard, ISO/IEC 20000, is adapted from ITIL.
- **ISO/IEC 38500:** This international standard on corporate governance of IT is suitable for small and large organizations in the public or private sector.
- **COSO:** This framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission to combat internal fraud. COSO is a framework of internal controls, mainly targeting financial accounting systems and implicitly underlying relevant IT controls.

These and other frameworks are discussed in greater detail in Appendix A.

Digital Transformation

The phenomenon known as digital transformation represents the trend of increasing reliance of businesses on information technology. DX, as it is sometimes known, surpasses the mere support of business processes with information technology, but also includes business processes entirely based on IT. This trend underscores the need for information system (IS) auditors, and even the digital transformation of IS auditing itself.

IT Strategy Committee

In organizations where IT plays a significant strategic business role, the board of directors should have an IT strategy committee, consisting of members of the board who have experience in technology issues. This group will advise the full board of directors on strategies to enable better IT support of the organization's overall strategy and objectives.

The IT strategy committee can meet with the organization's top IT executives to impart the board's wishes directly to them. This works best as a two-way conversation, where IT executives can inform the strategy committee of their status on major initiatives, as well as on challenges and risks. This ongoing dialogue can take place as often as needed, usually once or twice a year.

Readers should note that this suggestion of the IT strategy committee communicating with IT management is not an attempt to circumvent communications through intermediate layers of management. Those individuals should be included in this conversation as well.

The Balanced Scorecard

The *balanced scorecard (BSC)* is a management tool that is used to measure the performance and effectiveness of an organization. The BSC is used to determine how well an organization can fulfill its mission and strategic objectives, and how well it is aligned with overall organizational objectives.

In the BSC, management defines key performance indicators (KPIs) in each of four perspectives:

- **Financial:** Key financial items measured include the cost of strategic initiatives, support costs of key applications, and investment.
- **Customer:** Key measurements include the satisfaction rate with various customer-facing aspects of the organization.
- **Internal business:** Measurements of activities that the organization must perform as the essential components of the business that drive customer satisfaction.
- **Innovation and learning:** Measurements of activities that drive the company's future success, including new product development and continuous product improvement.

Each organization's BSC will represent a unique set of measurements that reflects the organization's type of business, business model, and style of management.

The Standard IT Balanced Scorecard

The BSC should be used to measure overall organizational effectiveness and progress. A similar scorecard, the standard IT balanced scorecard (IT-BSC), can be used specifically to measure IT organization performance and results.

Like the BSC, the standard IT-BSC has four perspectives:

- **Business contribution:** Key indicators here are the perception of IT department effectiveness and value as seen from other (non-IT) corporate executives.
- **User:** Key measurements include end-user satisfaction rate with IT systems and the IT support organization. Satisfaction rates of external users should be included if the IT department builds or supports externally facing applications or systems.
- **Operational excellence:** Key measurements include the number of support cases, amount of unscheduled downtime, and defects reported.
- **Innovation:** This includes the rate at which the IT organization uses newer technologies to increase IT value and the amount of training made available to IT staff.

The IT-BSC should flow directly out of the organization's overall BSC. This will ensure that IT will align itself with corporate objectives. Although the perspectives between the overall BSC and the IT-BSC vary, the approach for each is similar, and the results for the IT-BSC can "roll up" to the organization's overall BSC.

Information Security Governance

Security governance is the collection of management activities that establishes key roles and responsibilities, identifies and treats risks to key assets, and measures key security processes. Depending on the structure of the organization and its business purpose, information security governance may be included in IT governance, or security governance may stand on its own (but if so, it should still be linked to IT governance so that these two activities are kept in sync). Security governance helps to align information security with the organization's strategies and objectives.

The main roles and responsibilities for security should be as follows:

- **Board of directors:** The board is responsible for establishing the tone for risk appetite and risk management in the organization. To the extent that the board of directors establishes business and IT security, so, too, should the board consider risk and security in that strategy. The board is accountable to shareholders for the overall performance of the firm, including the satisfaction of information security obligations.
- **Steering committee:** The security steering committee should establish the operational strategy for security and risk management in the organization. This includes setting strategic and tactical roles and responsibilities in more detail than was done by the board of directors. The security strategy should be in harmony with the strategy for IT and the business overall. The steering committee should also ratify security policy and other strategic policies and processes developed by the chief information security officer.
- **Chief information security officer (CISO):** The CISO should be responsible for developing security policy; conducting risk assessments; developing processes for risk management, vulnerability management, incident management, identity and access management, security awareness and training, third-party risk management, and

compliance management; and informing the steering committee and board of directors of incidents and new or changed risks. In some organizations, this is known as the chief information risk officer (CIRO).

Some organizations may employ a chief security officer (CSO) who is responsible for logical security as described in the CISO role, as well as physical security, including workplace and personnel safety, physical access control, and investigations.

- **Chief information officer (CIO):** The CIO is responsible for overall leadership of the IT organization, including IT strategy, development, operations, and service desk. In some organizations the CISO or another top-ranking security individual reports to the CIO, while in other organizations they are peers.
- **Management:** Every manager in the organization should be at least partially responsible for the conduct of their employees. This approach helps to establish a chain of accountability from the top of the organization all the way down to individual employees.
- **Internal audit:** Internal auditors are responsible for providing independent and objective assurance that the organization is achieving its stated objectives.
- **All employees:** Every employee in the organization should be required to comply with the organization's security policy, as well as with security requirements and processes. All senior and executive management personnel should demonstrably comply with these policies as an example for others.

Security governance is not only for the identification and enforcement of applicable laws, regulations, and other legal requirements, but also for the fulfillment of goals and objectives, as well as management, monitoring, and enforcement of policies and processes.

Security governance should also make it clear that compliance with policies is a condition of employment; employees who fail to comply with policy are subject to discipline or termination of employment.

Where Should the CISO Report?

A great debate rages on in the cybersecurity community about where the CISO should fit within an organization. Some argue that the CISO should report to the CIO, while others insist they be peers reporting to the CEO. While there is no right answer for all organizations, many organizations choose to divide security responsibilities. In such an arrangement, the CISO might oversee governance, policy, investigations, and risk. The CIO may oversee a security operations function that carries out daily operational tasks. This approach has the benefit of allowing the CISO to oversee governance efforts with independence from the IT organization while the CIO can lead a team responsible for end-to-end technical operations.

Reasons for Security Governance

Organizations are dependent on their information systems. This has progressed to the point where organizations—including those whose products or services are not information-related—are completely dependent on the integrity and availability of their information systems to continue operations; this is the trend of digital transformation. Security governance, then, is needed to ensure that the probability and impact of security-related incidents are minimized and do not threaten critical systems and their support of the ongoing viability of the organization.

Security Governance Activities and Results

Within an effective security governance program, the organization's management will see to it that information systems necessary to support business operations will be adequately protected. Following are some of the activities that will take place:

- **Risk management:** Management will ensure that risk assessments will be performed to identify risks in information systems. Follow-up actions—primarily, risk treatment—will be carried out that will reduce the risk of system failure and compromise to acceptable levels that align with the organization's risk appetite or risk tolerance.
- **Process improvement:** Management will ensure that key changes will be made to business processes that will result in security improvements.
- **Incident response:** Management will implement incident response procedures that will help to avoid incidents, reduce the impact and probability of incidents, and improve response to incidents so that their impact on the organization is minimized.
- **Improved compliance:** Management will be sure to identify all applicable laws, regulations, and standards and carry out activities to confirm that the organization is able to attain and maintain compliance.
- **Business continuity and disaster recovery planning:** Management will define objectives and allocate resources for the development of business continuity and disaster recovery plans.
- **Third-party risk management:** With increased reliance on external service providers, management will direct the assessment and management of third-party service providers that process and store critical information and perform critical functions for the organization.
- **Effectiveness measurement:** Management will establish processes to measure key security events such as incidents, policy changes and violations, audits, and training.
- **Resource management: The** allocation of labor, budget, and other resources to meet security objectives will be monitored by management.
- **Improved IT governance:** An effective security governance program will result in better strategic decisions in the IT organization that keep risks at an acceptably low level.

These and other governance activities are carried out through planned interactions among key business and IT executives at regular intervals. Meetings will include a discussion of effectiveness measurements, recent incidents, recent audits, and risk assessments. Other discussions may include such things as changes to the business, recent business results, and any anticipated business events such as mergers or acquisitions.

There are two key results of an effective security governance program:

- **Increased trust:** Customers, suppliers, and partners trust the organization to a greater degree when they see that security is managed effectively.
- **Improved reputation:** The business community, including customers, investors, and regulators, will hold the organization in higher regard.

IIA Three-Lines Model

The Institute of Internal Auditors (IIA) uses a three-lines model to describe how assurance and governance exist in an organization.

In this model, the board of directors is accountable to stakeholders for overseeing the organization. The board delegates responsibility to both management and the internal audit department.

Management is responsible for taking actions to manage risk and achieve the organization's objectives. Management reports to the board and coordinates with the internal audit department.

Internal audit is responsible for providing independent assurance. The internal audit department also reports to the board and coordinates with management.

IT Strategic Planning

A good strategic planning process answers the question of what should we do? Although IT organizations require personnel who perform the day-to-day work of supporting systems and applications, some IT personnel need to spend at least part of their time developing plans for what the IT organization will be doing two, three, or even five years into the future.

Strategic planning needs to be part of a formal, iterative planning process, not an ad hoc, chaotic activity. Specific roles and responsibilities for planning need to be established, and those individuals must carry out planning roles as they would any other responsibility. A part of the struggle with the process of planning stems from the fact that strategic planning is partly a creative endeavor that includes analysis of reliable information about future technologies and practices, as well as a development of long-term strategic plans for the organization itself.

In a nutshell, the key question is this: In five years, when the organization will be performing specific activities in a particular manner, how will IT systems enable and support those activities?

But it's more than just understanding how IT will support future business activities. Innovations in IT may help to shape what activities will take place, or at least how they will take place. On a more down-to-earth level, IT strategic planning is about the ability to provide the capability and capacity for IT services that will match the levels of and the types of business activities that the organization expects to achieve at certain points in the future. In other words, if organizational strategic planning predicts specific transaction volumes (as well as new types of transactions) at specific points in the future, the job of IT strategic planning will be to ensure that cost-effective IT systems of sufficient processing capacity will be up and running to support those features and workloads. As digital transformation sweeps across industries, increasingly, IT does not merely support a business process; IT is a business process.

Discussion of new business activities, as well as the projected volume of current activities at certain times in the future, is most often discussed by a steering committee.

The IT Steering Committee

A *steering committee* is a body of senior managers or executives that meets from time to time to discuss high-level and long-term issues in the organization. An IT steering committee will typically discuss the future state of the organization and how the IT organization will evolve to meet the organization's needs. A steering committee will typically consist of senior-level IT managers as well as business unit leaders, and key internal customers or constituents. This provider-customer dialogue will help to ensure that IT, as the organization's technology service arm, will fully understand the future vision of the business (in business terms) and be able to support future business activities in terms of capacity, cost-effectiveness, and the ability to support new activities that do not yet exist.

The IT steering committee also assesses results of recent initiatives and major projects to gain a high-level understanding of past performance in order to shape future activities. The committee also needs to consider industry trends and practices, risks as defined by internal risk assessments, and current IT capabilities.

The role of the IT steering committee is depicted in Figure 1.1.

A steering committee's mission, objectives, roles, and responsibilities should be formally defined in a written charter. Steering committee meetings should be documented and minutes published.

The steering committee needs to meet regularly to consider strategic issues and make decisions that translate into actions, tasks, and projects in IT and elsewhere.

FIGURE 1.1 The IT steering committee synthesizes a future strategy using several inputs.

Not all organizations have an IT steering committee. The role is sometimes filled by key senior staff members, with or without an official charter. And in some organizations, the role is not filled at all; as a result, the IT organization is more likely to be directionless and not aligned to the business.

The IT steering committee differs from the IT strategy committee discussed earlier. The steering committee is an internal committee consisting of managers and other stakeholders who are employees of the organization. The strategy committee is a committee of the board of directors.

Policies, Processes, Procedures, and Standards

Policies, processes, procedures, and standards define IT organizational behavior and uses of technology. They are part of the written record that defines how the IT organization performs the services that support the organization.

Policy documents should be developed and ratified by IT management and should be reviewed annually. Policies state only what must be done (or not done) in an IT organization. They should not state how something must be done (or not done). That way, a policy document will be durable—meaning it may last many years with only minor edits from time to time.

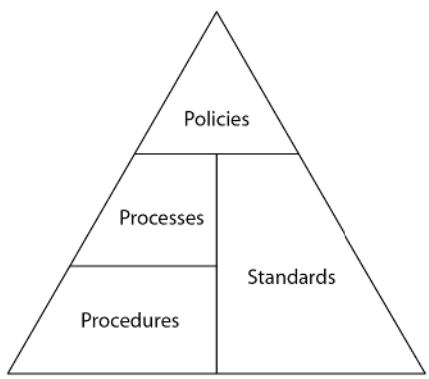
IT policies typically cover many topics, including the following:

- **Roles and responsibilities:** These will range from general to specific, usually by describing each major role and responsibility in the IT department and then specifying which position is responsible for it. IT policies will also make general statements about responsibilities that all IT employees will share.
- **Development and acquisition practices:** IT policy should define the processes used to acquire, develop, and implement software for the organization. Typically, IT policy will require a formal development methodology that includes a few specific ingredients, such as quality review and the inclusion of security requirements and testing.
- **Operational practices:** IT policy defines the high-level processes that constitute IT's operations. This will include service desk, backups, system monitoring, metrics, and other day-to-day IT activities.
- **IT processes, documents, and records:** IT policy will define other important IT processes, including incident management, project management, vulnerability management, and support operations. IT policy should also define how and where documents such as procedures and records will be managed and stored.

IT policy, like any other organization policy, is generally focused on what should be done and on what parties are responsible for different activities. However, policy generally steers clear of describing how these activities should be performed. That, instead, is the role of procedures and standards, discussed later in this section.

The relationship between policies, processes, procedures, and standards is shown in Figure 1.2.

FIGURE 1.2 Policies, processes, procedures, and standards



Information Security Policy

The *information security policy* defines how an organization will protect its important assets and respond to threats and incidents. Like IT policy, information security policy defines several fundamental principles and activities:

- **Roles and responsibilities:** Security policy should define specific roles and responsibilities, including the roles of specific positions in the organization as well as the responsibilities of all staff members.
- **Risk management:** Security policy should define how the organization identifies, manages, and treats risks. An organization should perform periodic risk assessments and risk analysis, which will lead to decisions about risk treatment for specific risks that are identified, and which align with established risk tolerance levels.
- **Security processes:** Security policy should define important security processes, such as vulnerability management and incident management, and incorporate security into other business processes, such as software development and acquisition, vendor selection and management, and employee screening and hiring.
- **Acceptable use:** Security policy should define the types of activities and behaviors that are acceptable and those that are not.

The best practice for information security policy is the definition of a top-down, management-driven information security program that performs periodic risk assessments to identify and focus on the most important risks in the organization. Roles and responsibilities define who is responsible for carrying out these activities. Executive management should have visibility and decision-making power, particularly in the areas of policy review and risk treatment.

It is generally accepted that security policy and security management should be separate from IT policy and IT management. This permits the security organization function to operate outside of IT, thereby permitting security to be objective and independent of IT. This puts security in a better position to be able to assess IT systems and processes objectively without fear of direct reprisal.

Privacy Policy

One of the most important policies an organization will develop that is related to information security is a privacy policy. A privacy policy describes how the organization will treat personally identifiable information (PII). PII is information that is considered private because it can be tied to a specific person, such as full name, address, and Social Security number. A privacy policy defines two broad activities in this regard:

- **Protecting private information:** An organization that is required to collect, store, or transmit PII is duty-bound to protect this information so that it is not disclosed to unauthorized parties. This part of the privacy policy will describe what information is obtained and how it is protected.

- **Handling private information:** Aside from the actual protection of PII, some organizations may, in the course of their business activities, transmit some or all of this information to other parts of the organization or to other organizations. A privacy policy is typically forthright about this internal handling and sharing with third parties. Further, a privacy policy describes how the information is used by the organization and by other organizations to which it is transmitted. The privacy policy typically describes how a private citizen may confirm whether their PII is stored by the organization, whether it is accurate, and how the citizen can arrange for its removal if they wish.

Many countries have privacy laws that require an organization to have a privacy policy and to enact safeguards to protect private information.

Data Classification Policy

A *data classification policy* defines degrees of sensitivity for various types of information used in the organization. A typical data classification policy will define two or more (but rarely more than five) data classification levels, such as the following:

- Top Secret
- Secret
- Sensitive
- Public

Along with defining levels of classification, a data classification policy will define policies and procedures for handling information in various settings at these levels. For instance, a data classification policy will state the conditions at each level in which sensitive information may be emailed, faxed, stored, transmitted, or shipped. Note that some methods for handling may be forbidden, such as emailing a Top Secret document over the Internet.

Leaders should ensure that the data classification program and practices align with the organization's data governance program, privacy program, policies, and applicable external requirements.

Exam Tip

While the CISO is responsible for establishing the organization's data classification policy, it is usually the responsibility of a document owner to classify and mark a document correctly. It is then the responsibility of any party who uses a document to handle it according to its classification level. All personnel who work with the document are responsible for handling it according to the classification policy.

System Classification Policy

A data classification policy may specify levels of security for systems storing classified information. A system classification policy will establish levels of system security that correspond to levels of data classification. Such a policy will help the organization to be more deliberate in its system hardening standards so that the most sensitive information will be stored only on systems with the highest levels of hardening (often, those higher levels of hardening are more costly and time-consuming to manage; otherwise, an organization might just make all of its systems highly sensitive).

Site Classification Policy

A *site classification policy* defines levels of security for an organization's work sites. This policy sets levels of physical security that correspond to one or more factors:

- Criticality of staff who work at the site
- Criticality or value of business processes performed at the site
- Value of assets located at the site
- Sensitivity or value of data stored or processed at the site
- Siting risks associated with a site (human-made or natural hazards)

Based on the classification of a site, an organization may have additional security controls, such as video surveillance, guards, fences, visitor controls, and so on. Just as it does not make sense to protect all data at a single level, it also is sensible to have the appropriate level of physical security at each site according to the information, equipment, or activity that takes place there.

Access Control Policy

An *access control policy* defines the need for specific processes and procedures related to the granting, review, and revocation of access to systems and work areas. This policy will state which roles are permitted to manage access controls, what levels of approval are required for access requests, how often access reviews will take place, and what access control records will be kept.

Often, there will be a linkage between a data classification policy and an access control policy. This is because access controls protecting the most sensitive information should usually be stricter than access controls protecting less sensitive information.

Mobile Device Policy

A *mobile device policy* defines the use of mobile devices and personally owned devices in the context of business operations and access to business information and information systems. This policy will state the types of devices that may be permitted, the rules and conditions of

their use, and the responsibilities of device owners and users. A mobile device policy often addresses the business rules related to the use of bring your own device (BYOD) that allow employees to use personally owned devices such as smartphones to access and manage business information.

Social Media Policy

A *social media policy* defines employees' use of social media. Generally, this encompasses online behavior and employees' online representations of their personal and professional conduct. A social media policy may include the following components:

- **Personal social media:** Policy may limit the posting of content that could put the employee or the organization in a bad light.
- **Professional social media:** Policy may address or restrict how employees describe their positions and activities in the workplace.
- **Disclosure of company information:** Policy may restrict the types of information that employees are permitted to disclose to the public.

Although organizations generally don't try to restrict employees' use of social media, organizations use social media policy to reaffirm their ownership of official information about the organization.

Other Policies

Organizations may have additional technology-related policies, including the following:

- **Equipment control and use:** Policy may address the appropriate use of IT and other equipment, perhaps including equipment assigned to employee use in the field.
- **Data destruction:** Policy defines acceptable and required methods for the disposal of information when it's no longer needed.
- **Moonlighting:** Policy addresses matters regarding outside employment, such as employees who have a second job or who perform volunteer work.
- **Intellectual property:** Policy addresses matters related to the ownership of intellectual property that is created, accessed, or used.
- **Use of portable storage devices:** Policy addresses the use of portable storage devices to prevent the removal of sensitive information from the organization or the introduction of malware.

Processes and Procedures

Process and procedure documents, sometimes called standard operating procedures (SOPs), describe in step-by-step detail how IT processes and tasks are performed. Formal procedure

documents ensure that tasks are performed consistently and correctly, even when performed by different IT staff members.

In addition to the actual steps in support of a process or task, a procedure document needs to contain several pieces of metadata:

- **Document (or process) ownership:** The document should contain the name of the person or department responsible for its review, revision, and publication.
- **Document revision information:** The procedure document should contain the name of the person who wrote the document and the person who made the most recent changes to the document. The document should also include the name or location where the official copy of the document can be found.
- **Review and approval:** The document should include the name of the manager who last reviewed the procedure document, as well as the name of the manager (or higher) who approved the document.
- **Dependencies:** The document should specify which other procedures are related to each procedure. This includes other procedures that are dependent on a procedure, and any other procedures that each procedure depends on. For example, a document that describes the database backup process will depend on database management and maintenance documents; documents on media handling will depend on this document.

IT process and procedure documents are not meant to be a replacement for vendor task documentation. For instance, an IT department does not necessarily need to create a document that describes the steps for operating a data storage device when the device vendor's instructions are available and sufficient. Also, IT procedure documents need not be remedial and include every specific keystroke and mouse click; they can usually assume that the reader has experience in the subject area and needs to know how things are done in this organization only. For example, a procedure document that includes a step that involves the modification of a configuration file does not need to include instructions on how to operate a text editor.

An IT department should maintain a catalog of its procedure documents to facilitate convenient document management. This will permit IT management to better understand which documents are in its catalog, when each was last reviewed and updated, and which will be impacted by specific IT or business changes.

Standards

IT standards are official, management-approved statements that define the technologies, protocols, suppliers, and methods that are used by an IT organization. Standards help drive consistency across the IT organization, which will make the organization more cost-efficient and cost-effective.

An IT organization will have different types of standards, including these:

- **Technology/product standards:** These standards specify what software and hardware technologies or products are used by the IT organization. Examples include operating systems, database management systems, application servers, storage systems, backup media, and so on.
- **Protocol standards:** These standards specify the protocols that are used by the organization. For instance, an IT organization may opt to use Transmission Control Protocol/Internet Protocol (TCP/IP) v6 for its internal networks, Cisco gateway routing protocols (GRPs), Transport Layer Security (TLS) for secure transmission of data, Secure Shell (SSH) for device management, and so forth.
- **Supplier standards:** These define which suppliers and vendors are used for various types of supplies and services. Using established suppliers can help the IT organization through specially negotiated discounts and other arrangements.
- **Methodology standards:** These refer to practices used in various processes, including software development, system administration, network engineering, and end-user support.
- **Configuration standards:** These standards refer to specific detailed configurations that are to be applied to servers, database management systems, end-user workstations, network devices, and so on. This enables users, developers, and technical administrative personnel to be more comfortable with IT systems, because the systems will be consistent with one another. This helps reduce unscheduled downtime and improves quality.
- **Architecture standards:** These standards refer to the technology architecture at the database, system, or network level. An organization may develop reference architectures for use in various standard settings. For instance, a large retail organization may develop specific network diagrams to be used in every retail location, down to the colors of wires to use and how equipment is situated on racks or shelves.
- **Security standards:** These standards apply to security-specific technologies, mechanisms, and controls. Examples include encryption algorithm or strength, password complexity, or requirements for multifactor authentication. The standards ensure that an organization meets the requirements to protect information, ensure compliance with governance, and reduce risk.

Standards enable the IT organization to be simpler, leaner, and more efficient. IT organizations with effective standards will have fewer types of hardware and software to support, which reduces the number of technologies that must be managed by the organization. An organization that standardizes on one operating system, one database management system, and one server platform need only build expertise in those technologies. This enables the IT organization to manage and support the environment more effectively than if many different technologies were in use.

Enterprise Architecture

Enterprise architecture (EA) is both a business function and a technical model. In terms of a business function, the establishment of an EA consists of activities that ensure that important business needs are met by IT systems overall. EA may also involve the construction of a model that is used to map business functions into the IT environment and IT systems in increasing levels of detail so that IT professionals can more easily understand the organization's technology architecture at any level.

The Zachman Framework

The *Zachman* enterprise architecture framework, established in the late 1980s, continues to be the dominant EA standard today. Zachman likens IT EA to the construction and maintenance of an office building: at a high (abstract, not number of floors) level, the office building performs functions such as containing office space. As we look into increasing levels of detail in the building, we encounter various trades (steel, concrete, drywall, electrical, plumbing, telephone, fire control, elevators, and so on), each with its own specifications, standards, regulations, construction and maintenance methods, and so on.

In the Zachman framework, IT systems and environments are described at a high, functional level, and then in increasing detail, encompassing systems, databases, applications, networks, and so on. The Zachman framework is illustrated in Table 1.1.

TABLE 1.1 Zachman framework showing IT systems in increasing levels of detail

	Data	Functional (Application)	Network (Technology)	People (Organization)	Time	Strategy
Scope	List of datasets important in the business	List of business processes	List of business locations	List of organizations	List of events	List of business goals and strategy
Enterprise Model	Conceptual data/object model	Business process model	Business logistics	Workflow	Master schedule	Business plan
Systems Model	Logical data model	System architecture	Detailed system architecture	Human interface architecture	Processing structure	Business rule model
Technology Model	Physical data/class model	Technology design	Technology architecture	Presentation architecture	Control structure	Rule design
Detailed Representation	Data definition	Program	Network architecture	Security architecture	Time definition	Rule speculation
Function Enterprise	Usable data	Working function	Usable network	Functioning organization	Implemented schedule	Working strategy

While the Zachman framework enables an organization to peer into cross-sections of an IT environment that support business processes, the model does not convey the relationships between IT systems. Data flow diagrams, discussed in the next section, are instead used to depict information flows.

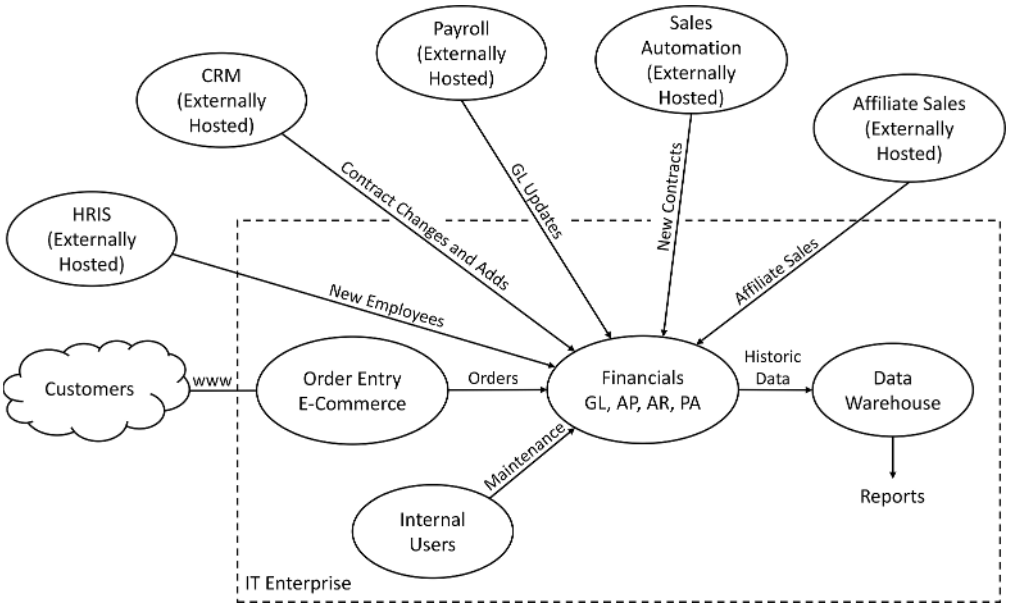
The U.S. government takes EA quite seriously. All U.S. government agencies are required to develop EA and use it in their strategic planning activities. Often the DoD Architecture Framework (DoDAF) is used for this purpose.

Data Flow Diagrams

Data flow diagrams (DFDs) are frequently used to illustrate the flow of information between IT applications. Like the Zachman model, a DFD can begin as a high-level diagram, where the labels of information flows are expressed in business terms. Written specifications about each flow can accompany the DFD; these specifications would describe the flow in increasing levels of detail, all the way to field lengths and communication protocol settings.

Similar to Zachman, DFDs enable nontechnical business executives to understand the various IT applications and the relationships between them. A typical DFD is shown in Figure 1.3.

FIGURE 1.3 A typical DFD shows the relationship between IT applications.



Data Storage Diagrams

A counterpart to data flow diagrams are depictions (visual or tabular) or data storage diagrams. These depict data at rest across the enterprise. The purpose of data storage diagrams (or data storage catalogs) is to document the intended and expected instances of stored information in the organization.

Data storage diagrams document the structured data that resides in an organization. The term "structured data" refers to the fact that data in this instance resides in formal management systems (often, database management systems, or DBMSs) that have a structured design, usually known as a schema. Contrast structured data to unstructured data, which is the data that resides in network file shares and end-user workstations in a mostly or entirely ad hoc fashion. Unstructured data often exists as a result of the ability of business applications to produce extracts and reports, which users create, download, and store on their local workstations or on network file shares.

Zero Trust

Zero trust is an architectural philosophy wherein one or more portions of an environment are considered untrusted. The first such model is the greater Internet itself: networks and workstations external to an organization (on the Internet) are not controlled by the organization and, hence, are untrusted. This model applies not only to the technology in place, but also to the intent of the people using that technology (consider hackers and cybercriminal organizations).

The zero trust model is increasingly being used by organizations in various contexts. Consider, for instance, an organization with a traditional data center and office networks with end-user computing. An organization may adopt a zero trust model with respect to the relationship between the information systems and applications in its data center, and its workstations. The design of its data centers, information systems, and applications assumes that the entire set of end-user systems are untrusted (which is rarely the actual case, but stay with me here). This thought process gives rise to a different way of thinking about security controls protecting the data center with its applications; if one assumes that an organization's end-user computing environment is like the Internet itself (completely untrusted), then this naturally gives rise to more rigorous protection of the data center environment by protecting it from all endpoints, including those managed by the organization.

This is an entirely valid approach. In many organizations, end users are permitted to change the configuration of their workstations, and they are sometimes permitted to use their own workstations. Further, consider the threat and effect of malware, which often strikes end-user workstations, and the additional threat therein. Given these conditions, it is often prudent to apply protective controls to a data center as though all end-user workstations were uncontrolled and untrusted (because, often, that is exactly the case).

Zero trust principles apply in other instances as well. The result is generally the same: Communications between one environment (or system) and another must be verified in various ways to ensure that no unplanned or hostile activities can interfere with computing and business operations.

Applicable Laws, Regulations, and Standards

Organizations need to identify all of the laws, regulations, and standards that are applicable to their operations. As IT has become more critical for organizations in many industry sectors, many nations and local governments have enacted new laws and regulations concerning the processing and protection of information.

The board of directors, strategy committee, or chief legal counsel should appoint an executive to be responsible for identifying all potentially applicable laws, regulations, and standards. This appointee should then consult with inside or outside legal counsel to determine their scope and applicability.

Once applicable laws and regulations have been identified, the organization needs to determine how they affect the following:

- **Enterprise architecture:** Laws, regulations, and standards may require that organizations use specific IT components or configurations that affect the organization's EA.
- **Controls:** Laws and regulations may require that additional controls be enacted or existing controls be changed.
- **Business processes:** Laws and regulations may require that the organization perform certain tasks that may affect processes.
- **Personnel:** Laws and regulations may require that certain personnel possess specific qualifications, certifications, or licenses.

Many factors will determine whether specific requirements are applicable to an organization, including these:

- Type of data that is stored, processed, or transmitted by the organization's systems
- Industry sector
- Location and management of stored, processed, or transmitted data
- Location of the owner(s) and steward(s) of stored, processed, or transmitted data

Organizations may also be required to comply with specific standards. For example, organizations that process, store, or transmit payment card numbers may be required to comply with the Payment Card Industry Data Security Standard (PCI DSS), even though there may be no laws requiring organizations to do so.

Risk Management

Organizations need to understand the internal activities, practices, and systems, as well as threats, that are introducing risk into their operations. The span of activities that seek, identify, and manage these risks is known as risk management. Like many other processes, risk management is a life cycle activity that has no beginning and no end. It's a continuous and phased set of activities that includes the examination of processes, records, systems, and

external phenomena in order to identify risks. This is continued by an analysis that examines a range of solutions for reducing risk, followed by formal decision making that brings about a resolution to risks.

Risk management needs to support the overall business objectives. This support will include the adoption of a risk appetite that reflects the organization's overall approach to risk. For instance, if the organization is a conservative financial institution, the organization's risk management program will probably adopt a position of being risk averse. Similarly, a high-tech startup organization that, by its very nature, is comfortable with overall business risk will probably be less averse to risks identified in its risk management program.

Regardless of its overall risk appetite, when an organization identifies risks, the organization can take one of four possible actions:

- **Accept:** The organization accepts the risk as is.
- **Mitigate (or reduce):** The organization acts to reduce the level of risk.
- **Transfer (or share):** The organization shares the risk with another entity, often an insurance company.
- **Avoid:** The organization discontinues the activity associated with the risk.

These choices are known as risk treatments. Often, a particular risk will be treated with a blended solution that consists of two or more of the actions just listed.

This section dives into the details of risk management, risk analysis, and risk treatment.

Governance, Risk, and Compliance

Governance, risk, and compliance (GRC) is an integrated approach that ensures organizations achieve their objectives, manage uncertainty, and act with integrity. It encompasses three interrelated disciplines: governance, risk management, and compliance.

Governance refers to the frameworks, policies, and procedures that senior management and the board of directors use to exert strategic control over business operations. It ensures that IT aligns with the organization's goals and objectives. Effective governance involves establishing clear roles and responsibilities, setting objectives, monitoring performance, and ensuring accountability.

Risk management involves identifying, assessing, and prioritizing risks followed by coordinated efforts to minimize, monitor, and control the probability or impact of unfortunate events. The goal is to ensure that risks are managed within the organization's risk appetite.

Compliance ensures that an organization adheres to legal, regulatory, and industry standards. It involves not only meeting external requirements but also adhering to internal policies and procedures.

The Risk Management Program

An organization that operates a risk management program should establish principles that will enable the program to succeed. These may include the following:

Objectives The risk management program must have a specific purpose; otherwise, it will be difficult to determine whether the program is successful. Example objectives include reducing the number of industrial accidents, reducing the cost of insurance premiums, and reducing the number or severity of security incidents. If objectives are measurable and specific, then the individuals who are responsible for the risk management program can focus on its objectives to achieve the best possible outcome.

Scope Management must determine the scope of the risk management program. This is a delicate undertaking because of the many interdependencies found in IT systems and business processes. However, in an organization with several distinct operations or business units (BUs), a risk management program could be isolated to one or more operational arms or BUs. In such a case, where there are dependencies on other services in the organization, those dependencies can be treated like external service providers (or customers).

Authority The risk management program is formally authorized or led by one or more executives in the organization. It is important to know who these individuals are and their levels of commitment to the program.

Roles and Responsibilities The program clearly identifies the specific job titles involved in risk management along with their respective roles and responsibilities. It should be clear which individuals are responsible for which activities in the program.

Resources The risk management program, like other activities in the business, requires resources to operate. This will include a budget for salaries as well as for workstations, software licenses, and possibly travel.

Policies, Processes, Procedures, and Records The various risk management activities, such as asset identification, risk analysis, and risk treatment, along with some general activities such as recordkeeping, should be included in business records.

An organization's risk management program should be documented in a charter. A charter is a formal document that defines and describes a business program and becomes a part of the organization's record.

The risk management life cycle is depicted in Figure 1.4.

The Risk Management Process

Risk management is a life cycle set of activities used to identify, analyze, treat, and monitor risks. These activities are methodical and, as mentioned in the previous section, should be documented so that they will be performed consistently and in support of the program's charter and objectives.

FIGURE 1.4 The risk management life cycle

The risk management process is part of a larger risk framework, such as ISACA's Risk IT Framework, whose components are:

- **Risk governance:** This includes integration with the organization's enterprise risk management (ERM) process, the establishment and maintenance of a common risk view, and the ability to ensure that business decisions include the consideration of risk.
- **Risk evaluation:** This includes asset identification, risk analysis, and the maintenance of a risk profile.
- **Risk response:** This includes the management and articulation of risks and the response to events.

Exam Tip

CISA candidates are not required to memorize the Risk IT Framework, but familiarity with its principles is important.

Asset Identification

The risk management program's main objective (whether formally stated or not) is the protection of the organization and its assets. These assets may be tangible or intangible, physical, logical, or virtual. Some examples of assets include the following:

- **Buildings and property:** These assets include structures and other improvements.
- **Equipment:** This can include machinery, vehicles, and office equipment such as copiers and fax machines.
- **IT equipment:** This includes computers, printers, scanners, tape libraries (the devices that create backup tapes, not the tapes themselves), storage systems, network devices, and phone systems.

- **Supplies and materials:** These can include office supplies as well as materials that are used in manufacturing.
- **Records:** These include business records, such as contracts, video surveillance tapes, visitor logs, and much more.
- **Information:** This includes data in software applications, documents, email messages, and files of every kind on workstations and servers.
- **Intellectual property:** This includes an organization's trade secrets, designs, architectures, software source code, processes, and procedures.
- **Personnel:** In a real sense, an organization's personnel are the organization. Without its staff, the organization cannot perform or sustain its processes.
- **Reputation:** One of the intangible characteristics of an organization, reputation is the individual and collective opinion about an organization in the eyes of its customers, competitors, shareholders, and the community.
- **Brand equity:** Similar to reputation, this is the perceived or actual market value of an individual brand of product or service that is produced by the organization.

Grouping Assets

For risk management purposes, an electronic inventory of assets will be useful in the risk management life cycle. It is not always necessary to list each individual asset; often, it is acceptable to instead list classes or groups of assets as a single asset entity for risk management purposes. For instance, a single entry for laptop computers may be preferred over listing every laptop computer; this is because the risks for all laptop computers are roughly the same (ignoring behavior differences among individual employees or employees in specific departments). This eliminates the need to list them individually.

Similarly, groups of IT servers, network devices, and other equipment can be named instead of all of the individual servers and devices, again because the risks for each of them will usually be similar. One reason to create multiple entries for servers, however, might be their physical location or their purpose; servers in one location may have different risks than servers in another location, and servers containing high-value information will have different risks than servers that do not contain high-value information.

Sources of Asset Data

An organization that is undergoing its initial risk management cycle may need to build its asset database from scratch. Management will need to determine where this initial asset data will come from, such as the following:

- **Financial system asset inventory:** An organization that keeps all of its assets on the books will have a wealth of asset inventory information. It may not be entirely useful, however; asset lists often do not include the location or purpose of the asset and whether it is still in use. Correlating a financial asset inventory to assets in actual use may consume more effort than the other methods for creating the initial asset list.

However, for organizations that have a relatively small number of highly valued assets (for instance, a rock crusher in a gold mine or a mainframe computer), knowing the precise financial value of an asset is highly useful because the actual depreciated value of the asset is used in the risk analysis phase of risk management. Knowing the depreciated value of other assets is also useful, as this will figure into the risk treatment choices that will be identified later.

Financial records that indicate the value of an asset do not include the value of information stored on (or processed by) the asset or the revenue earned through operation of the asset (or the financial consequences of its loss).

- **Interviews:** Discussions with key personnel for purposes of identifying assets are usually the best approach. However, to be effective, several people usually need to be interviewed to be sure to include all relevant assets.
- **IT systems portfolio:** A well-managed IT organization will have formal documents and records for its major applications. Although this information may not encompass every single IT asset in the organization, it can provide information on the assets supporting individual applications or geographic locations.
- **Online data:** An organization with numerous IT assets (systems, network devices, and so on) can sometimes utilize the capability of local online data to identify those assets. For instance, a systems or network management system often includes a list of managed assets, which can be a good starting point when creating the initial asset list.
- **Asset management system:** Larger organizations may find it more cost-effective to use an asset management application dedicated to this purpose, rather than rely on lists of assets from other sources.

Organizations need to keep in mind that some information assets will physically reside in service provider environments (mainly, information assets). For example, cloud service providers may be a critical portion of the IT infrastructure and the assets that organizations have deployed in the cloud should be included in the inventory.

Collecting and Organizing Asset Data

It is rarely possible to take (or create) a list of assets from a single source. Rather, more than one source of information is often needed to be sure that the risk management program has identified at least the important, in-scope assets that it needs to worry about.

As a part of IT governance, management needs to determine which person or group is responsible for maintaining an asset inventory.

It is usually useful to organize or classify assets. This will help to get the assets under study into smaller chunks that can be analyzed more effectively. There is no single way to organize assets, but here are a few ideas:

- **Geography:** A widely dispersed organization may classify its assets according to their locations. This will aid risk managers during the risk analysis phase, since many risks are geographic-centric, particularly natural hazards. Mitigation of risks is often geography based; for instance, it's easier to put a fence around one data center than to put up fences around buildings in every location.
- **Business process:** Because some organizations rank the criticality of their individual business processes, it can be useful to group assets according to the business processes that they support. This helps in the risk analysis and risk treatment phases, because assets supporting individual processes can be associated with business criticality and treated appropriately.
- **Organizational unit:** In larger organizations, it may be easier to classify assets according to the organizational units they support.
- **Sensitivity:** Usually ascribed to information, sensitivity relates to the nature and content of that information. Sensitivity usually applies in two ways: to an individual, where the information is considered personal or private, and to an organization, where the information may be considered a trade secret. Sometimes sensitivity is somewhat subjective and arbitrary, but often it is defined in laws and regulations.
- **Regulation:** For organizations that are required to follow government or private regulation regarding the processing and protection of information, it will be useful to include data points that indicate whether specific assets are considered in scope for specific regulations. This is important because some regulations specify how assets should be protected, so it's useful to be aware of this during risk analysis and risk treatment.

There is no need to choose which of these methods will be used to classify assets. Instead, an IT analyst should collect several points of metadata about each asset (including location, process supported, and organizational unit supported). This will enable the risk manager to sort and filter the list of assets in various ways to better understand which assets are in a given location or which ones support a particular process or part of the business.

Organizations should consider managing information about assets in a fixed-assets application.

Risk Analysis

Risk analysis is the activity in a risk management program where individual risks are identified. A risk consists of the intersection of threats, vulnerabilities, probabilities, and impact. In its simplest terms, risk is described in the following formula:

$$\text{Risk} = \text{Probability} \times \text{Impact}$$

This means that the level of risk facing an organization is determined by how likely it is that the risk will occur (probability) and how bad the situation will be if it does occur (impact).

You can use this equation literally by calculating risk, which is known as quantitative risk analysis. You may use it conceptually to ensure that you are considering all subjective factors during a qualitative risk analysis.

Other definitions of risk include the following:

- The combination of the probability of an event and its consequence (source: ISACA Cybersecurity Fundamentals Glossary)
- The probable frequency and probable magnitude of future loss (source: "An Introduction to Factor Analysis of Information Risk (FAIR)," Risk Management Insight, LLC)
- The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization (Source: ISO/IEC 27005)

These definitions convey essentially the same message: The amount of risk is directly proportional to the probability of occurrence and the impact that a risk would have if realized.

A risk analysis consists of identifying threats and their impact of realization against each asset. It usually also includes a vulnerability analysis, where assets are studied to determine whether they are vulnerable to identified threats. The sheer number of assets may make this task appear daunting; however, threat and vulnerability analyses can usually be performed against groups of assets. For instance, when identifying natural and human-made threats against assets, it often makes sense to perform a single threat analysis against all of the assets that reside in a given location. After all, the odds of a volcanic eruption are the same for any of the servers in the room—the threat need not be called out separately for each asset.

Threat Analysis

The usual first step in a risk analysis is to identify threats against an asset or group of assets. A threat is an event that, if realized, would bring harm to an asset and, hence, to the organization. Often called threat modeling, a typical approach is to list all of the threats that have some realistic opportunity of occurrence; those threats that are highly unlikely to occur can be left out. For instance, the listing of meteorites, tsunamis in landlocked regions, and wars in typically peaceful regions will just add clutter to a risk analysis.

A more reasonable approach in a threat analysis is to identify all of the threats that a reasonable person would believe could occur, even if the probability is low. For example, include flooding when a facility is located near a river, hurricanes for an organization located along the southern or eastern coast (and inland for some distance) of the United States, or a terrorist attack in practically every major city in the world. All of these would be considered reasonable in a threat analysis.

It is important to include the entire range of both natural and human-made threats. The full list could approach or even exceed 100 separate threats. The categories of possible threats include these:

- **Severe storms:** These includes tornadoes, hurricanes, windstorms, ice storms, and blizzards.

- **Earth movement:** This includes earthquakes, landslides, avalanches, volcanoes, and tsunamis.
- **Flooding:** This includes both natural and human-made situations.
- **Disease:** This includes sickness outbreaks and pandemics, as well as quarantines that result.
- **Fire:** This includes forest fires, range fires, and structure fires, all of which may be natural or human-caused.
- **Labor:** This includes work stoppages, protests, and strikes.
- **Violence:** This includes riots, looting, terrorism, and war.
- **Malware:** This includes all kinds of viruses, worms, Trojan horses, rootkits, ransomware, and associated malicious software.
- **Hacking attacks:** These include automated attacks (think of an Internet worm that is on the loose) as well as targeted attacks by employees, former employees, or criminals.
- **Hardware failures:** These include any kind of failure of IT equipment or failures of related environmental equipment, such as heating, ventilation, and air conditioning (HVAC).
- **Software failures:** These can include any software problem that precipitates a disaster.
- **Utilities:** These include electric power failures, water supply failures, and natural gas outages, as well as communications outages.
- **Transportation:** This includes airplane crashes, railroad derailments, ship collisions, and highway accidents.
- **Hazardous materials:** This includes chemical spills. The primary threat here is direct damage by hazardous substances, casualties, and forced evacuations.
- **Criminal activity:** This includes extortion, embezzlement, theft, vandalism, sabotage, and hacker intrusion. Note that company insiders can play a role in these activities.
- **Errors:** These include mistakes made by personnel that result in disaster situations.

Alongside each threat that is identified, the risk analyst assigns a probability or frequency of occurrence. For a quantitative risk analysis, this will be a numeric value, expressed as a probability of one occurrence within a calendar year. For example, if the risk of a flood is 1 in 100, it would be expressed as 0.01, or 1 percent. In a qualitative risk analysis, probability is expressed as a ranking; for example, Low, Medium, and High; or it can be expressed on a subjective numeric scale ranking the probability from 1 to 5.

An approach for completing a threat analysis is to:

- **Perform a geographic threat analysis for each location:** This will provide an analysis on the probability of each type of threat against all assets in each location.
- **Perform a logical threat analysis for each type of asset:** This provides information on all of the logical (that is, not physical) threats that can occur to each asset type.

For example, the risk of malware on all assets of one type is probably the same, regardless of the assets' locations.

- **Perform a threat analysis for each highly valued asset:** This will help to identify any unique threats that may have appeared in the geographic or logical threat analysis, but with different probabilities of occurrence.

Threat Forecasting Data Is Sparse

One of the biggest problems with information security–related risk management is the lack of reliable data on the probability of many types of threats. While the probability of some natural threats can sometimes be obtained from local disaster response agencies, the probabilities of most other threats are difficult to predict accurately.

The difficulty in predicting security events sits in stark contrast to volumes of available data related to automobile and airplane accidents, as well as human life expectancy. In these cases, insurance companies have been accumulating statistics on these events for decades, and the variables (for instance, tobacco and alcohol use) are well-known. On the topic of cyber-related risk, there is a general lack of reliable data, and the factors that influence risk are not well-known from a statistical perspective. It is for this reason that risk analysis still relies on educated guesses for the probabilities of most events. But given the recent surge in popularity for cyber insurance, the availability and quality of cyberattack risk factors may soon be more accurately determined.

Vulnerability Identification

A vulnerability is a weakness or absence of a protective control that increases the probability of one or more threats occurring. A vulnerability analysis is an examination of an asset to discover weaknesses that could lead to a higher than normal rate of occurrence or potency of a threat.

Here are some examples of vulnerabilities:

- Missing or inoperative antivirus software
- Outdated and unsupported software in use
- Missing security patches
- Weak password settings
- Missing or incomplete audit logs
- Inadequate monitoring of event logs
- Weak or defective application session management

- Building entrances that permit tailgating
- Insufficient coverage of video surveillance

In a vulnerability analysis, the risk manager needs to examine the asset itself as well as all of the protective measures that are—or should be—in place to protect the asset from relevant threats.

Vulnerabilities are usually ranked by severity. Vulnerabilities are indicators that show the effectiveness (or ineffectiveness) of protective measures. For example, an antivirus program on a server that updates its virus signatures once per week might be ranked as a medium vulnerability, whereas the complete absence (or malfunction) of an antivirus program on the same server might be ranked as a high vulnerability. Severity is an indication of the likelihood that a given threat might be realized. This is different from impact, which is discussed later in this section.

Probability Analysis

For any given threat and asset, the probability that the threat will actually be realized needs to be estimated. This is often easier said than done, as there is a lack of reliable data on security incidents. A risk manager will need to perform some research and develop a best guess based on any available data.

Impact Analysis

A threat, when actually realized, will have some effect on the organization. Impact analysis is the study of estimating the impact of specific threats on specific assets.

In impact analysis, it is necessary for the analyst to understand the relationship between an asset and the business processes and activities that the asset supports. The purpose of impact analysis is to identify the impact on business operations or business processes. This is because risk management is not an abstract identification of abstract risks, but instead a search for risks that have real impact on business operations.

In an impact analysis, the impact can be expressed as a rating such as H-M-L (High-Medium-Low) or as a numeric scale, and it can also be expressed in financial terms. But what is also vitally important in an impact analysis is the inclusion of a statement of impact for each threat. Example statements of impact include "inability to process customer support calls" and "inability for customers to view payment history." Statements such as "inability to authenticate users" may be technically accurate, but they do not identify the business impact.

Because of the additional time required to quantify and develop statements of impact, impact analysis is usually performed only on the highest ranked threats on the most critical assets.

Qualitative Risk Analysis

A qualitative risk analysis is an in-depth examination of in-scope assets with a detailed study of threats (and their probability of occurrence), vulnerabilities (and their severity), and

statements of impact. The threats, vulnerabilities, and impact are all expressed in qualitative terms such as High-Medium-Low or in quasi-numeric terms such as a 1–5 numeric scale.

The purpose of qualitative risk analysis is to identify the most critical risks in the organization based on these rankings.

Qualitative risk analysis does not get to the issue of "how much does a given threat cost my business if it is realized?"—neither does it mean to do this. The value in a qualitative risk analysis is the ability to identify the most critical risks quickly without the additional burden of identifying precise financial impacts.

The individual(s) performing risk analysis may want to include threat–vulnerability pairing as well as asset–threat pairing. These techniques may help a risk analyst better understand the probability or impact of specific threats.

Organizations that do need to perform quantitative risk analysis often begin with qualitative risk analysis to determine the highest-ranked risks that warrant the additional effort of quantitative analysis.

Quantitative Risk Analysis

Quantitative risk analysis is a risk analysis approach that uses numeric methods to measure risk. Quantitative risk analysis offers statements of risk in terms that can be easily compared with the known values of their respective assets. In other words, risks are expressed in the same units of measure as most organizations' primary unit of measure: financial.

Despite this, quantitative risk analysis must still be regarded as an effort to develop estimates, not exact figures. Partly this is because risk analysis is a measure of events that may occur, not a measure of events that do occur.

Standard quantitative risk analysis involves the development of several figures:

- **Asset value (AV):** This is the value of the asset, which is usually (but not necessarily) the asset's replacement value.
- **Exposure factor (EF):** This is the financial loss that results from the realization of a threat, expressed as a percentage of the asset's total value. Most threats do not completely eliminate the asset's value; instead, they reduce its value. For example, if a construction company's $500,000 earth mover is destroyed in a fire, the equipment will still have salvage value, even if that is only 10 percent of the asset's value. In this case, the EF would be 90 percent. Note that different threats will have different impacts on EF, because the realization of different threats will cause varying amounts of damage to assets.
- **Single loss expectancy (SLE):** This value represents the financial loss when a threat is realized one time. SLE is defined as AV × EF. Note that different threats have a varied impact on EF, so those threats will also have the same multiplicative effect on SLE.
- **Annualized rate of occurrence (ARO):** This is an estimate of the number of times that a threat will occur per year. If the probability of the threat is 1 in 50, then ARO is

expressed as 0.02. However, if the threat is estimated to occur four times per year, then ARO is 4.0. Like EF and SLE, ARO will vary by threat.

- **Annualized loss expectancy (ALE):** This is the expected annualized loss of asset value due to threat realization. ALE is defined as SLE × ARO.

Risk managers should take extra care to develop the best possible estimate for ARO, based on whatever data is available. Sources for estimates include:

- History of event losses in the organization
- History of similar losses in other organizations
- History of dissimilar losses
- Best estimates based on available data

When the analyst is performing a quantitative risk analysis for a given asset, the ALE for all threats can be added together. The sum of all ALEs is the annualized loss expectancy for the total array of threats. A particularly high sum of ALEs would mean that a given asset is confronted with a lot of significant threats that are more likely to occur. But in terms of risk treatment, ALEs are better off left as separate and associated with their respective threats.

Developing Mitigation Strategies

An important part of risk analysis is the investigation of potential solutions for reducing or eliminating risk. This involves understanding specific threats and their impact (EF) and likelihood of occurrence (ARO). Once a given asset and threat combination has been baselined (i.e., the existing asset, threats, and controls have been analyzed to understand the threats as they exist at a given point in time), the risk analyst can then apply various hypothetical means for reducing risk, documenting each one in terms of its impact on EF and ARO.

For example, suppose a risk analysis identifies the threat of attack on a public web server. Specific EF and ARO figures have been identified for a range of individual threats. Now the risk analyst applies a range of fixes (on paper), such as an application firewall, an intrusion prevention system (IPS), and a patch management tool. Each solution will have a specific and unique impact on EF and ARO (these are all estimates, of course, just like the estimates of EF and ARO on the initial conditions); some will have better EF and ARO figures than others. Each solution should also be rated in terms of cost (financial or H-M-L) and effort to implement (financial or H-M-L).

Developing mitigation strategies is the first step in risk treatment, where various solutions are put forward, each with its cost and impact on risk.

While security analysts may have the responsibility for documenting vulnerabilities, threats, and risks, it is senior management's responsibility (through the security steering committee) to formally approve the treatment of risk. Risk treatment is discussed later in this chapter.

Risk Analysis and Disaster Recovery Planning

Disaster recovery planning (DRP) and business continuity planning (BCP) utilize risk analysis to identify risks that are related to business resilience and the impact of disasters. The risk analysis performed for DRP and BCP is the same risk analysis that is discussed in this chapter—the methods and approach are the same, although the overall objectives are somewhat different.

Business continuity planning and disaster recovery planning are discussed in detail in Chapter 6, "Business Continuity and Disaster Recovery."

High-Impact Events

The risk manager is likely to identify one or more high-impact events during the risk analysis. These events, which may be significant enough to threaten the very viability of the organization, require risk treatment that warrants executive management visibility and belongs in the categories of business continuity planning and disaster recovery planning. These topics are discussed in detail in Chapter 6.

Risk Treatment

When risks to assets have been identified through qualitative and/or quantitative risk analysis, the next step in risk management is to decide what to do about the identified risks. During risk analysis, one or more potential solutions may have been examined, along with their cost to implement and their impact on risk. In risk treatment, a decision about whether to proceed with any of the proposed solutions (or others) is needed.

Risk treatment pits available resources against the need to reduce risk. In an enterprise environment, not all risks can be mitigated, because there are not enough resources to treat them all. Instead, a strategy for choosing the best combination of solutions that will reduce risk by the greatest possible margin is needed. For this reason, risk treatment is often more effective when all the risks and solutions are considered together, instead of considering each one separately. Then they can be grouped, compared, and prioritized.

When risk treatment is performed at the enterprise level, risk analysts and technology architects can devise ways to bring about the greatest possible reduction in risk. This can be achieved through the implementation of solutions that will reduce many risks for many assets at once. For example, a firewall can reduce risks from many threats on many assets; this will be more effective than individual solutions for each asset.

So far, we have been talking about risk mitigation as if it were the only option available when handling risk. But there are actually four primary ways to treat risk: mitigation, transfer, avoidance, and acceptance. And there is always some leftover risk, called residual risk. These approaches are discussed next.

Risk Mitigation

Risk mitigation, or risk reduction, involves the implementation of some solution that will reduce an identified risk. For instance, the risk of advanced malware being introduced on to a server can be mitigated with advanced malware prevention software or a network-based IPS. Either of these solutions would constitute mitigation of this risk on a given asset, and either solution would effectively mitigate the risk depending on the enterprise-level resource allocation.

An organization usually decides to implement some form of risk mitigation only after performing some cost analysis to determine whether the reduction of risk is worth the expenditure of risk mitigation.

Back to the term solution, as mentioned here. Readers should not automatically think of new devices, systems, or features such as firewalls, IPSs, antivirus software, data loss prevention systems, or other hardware or software products. Instead, a solution may be as simple as an update to a written policy, a configuration change, or the modification of a firewall rule, or it may be as complex as network segmentation that could take many months to implement. A solution could also be to monitor the risk to assess what the appropriate response could be if the risk were to materialize in a significant quantitative or qualitative way (for instance, monitoring for key cybersecurity intrusions and then choosing to implement mitigating measures if the threat level increases).

Risk Transfer

Risk transfer, or risk sharing, means that some or all of the risk is being transferred to some external entity, such as an insurance company or business partner. When an organization purchases an insurance policy to protect an asset against damage or loss, the insurance company is assuming part of the risk in exchange for payment of insurance premiums.

The details of a cyber-insurance policy need to be carefully examined to ensure that any specific risk is transferable to the policy. Cyber-insurance policies typically have exclusions that limit or deny payment of benefits in certain situations. Additionally, cyber risk insurance or other insurance policies can be contingent on the underwritten entity having proper risk mitigation and control activities in place as defined in the policy.

Organizations considering cyber-insurance policies should carefully read the terms and conditions of such policies to ensure the selection of an appropriate policy. Some policies assume and require that the organization have specific measures in place. Further, policies have exclusions that must be well understood. Some organizations are denied benefits from malware attacks that insurance companies claim are acts of war, a common exclusion.

Risk Avoidance

In *risk avoidance*, the organization abandons the potential risk activity altogether, effectively taking the asset out of service so that the threat is no longer present. In another scenario, the

organization may decide that the risk of pursuing a given business activity is too great so that specific activity is completely avoided. This can sometimes be illustrated through organizational efforts to minimize the amount of old software or hardware within the IT environment by replacing it with newer equipment.

Organizations do not often back away completely from an activity because of identified risks. Generally, this avenue is taken only when the risk of loss is great and the perceived probability of occurrence is high.

Risk Acceptance

Risk acceptance occurs when management is willing to accept an identified risk as is, with no effort taken to reduce it. Risk acceptance also takes place (sometimes implicitly) for residual risk, after other forms of risk treatment have been applied. It is important through governance policies and procedures for the organization to have a consistent approach to risk acceptance.

Residual Risk

Residual risk is the risk that is left over from the original risk after some of the risk has been removed through mitigation or transfer. For instance, if a particular threat had a probability of 10 percent before risk treatment and 1 percent after risk treatment, the residual risk is that 1 percent left over. This is best illustrated by the following formula:

Original Risk – Mitigated Risk – Transferred Risk = Residual Risk

It is unusual for risk treatment to eliminate risk altogether; rather, various controls are implemented that remove some of the risk. Often, management implicitly accepts the leftover risk; however, it's a good idea to make that acceptance of residual risk more formal by documenting the acceptance in a risk management log or decision log.

Compliance Risk

Organizations that perform risk management are generally aware of the laws, regulations, and standards they are required to follow. For instance, U.S.-based banks, brokerages, and insurance companies are required to comply with the Gramm–Leach–Bliley Act (GLBA), and organizations that store, process, or transmit credit card numbers are required to comply with PCI DSS (Payment Card Industry Data Security Standard). Health care providers and insurers in the United States are required to comply with the Health Insurance Portability and Accountability Act (HIPAA). The European General Data Protection Regulation (GDPR) has an especially long reach, applying to organizations throughout the world that store and process personally identifiable information about European Union (EU) citizens.

GDPR, GLBA, HIPAA, PCI DSS, and other regulations often state in specific terms what controls are required in an organization's IT systems. This brings to light the matter of compliance risk. Sometimes, the risk associated with a specific control (or lack of a control) may be rated as a low risk, either because the probability of a risk event is low or because the impact of the event is low. However, if a given law, regulation, or standard requires that the control be enacted anyway, the organization must consider the compliance risk. The risk of noncompliance may result in fines or other sanctions against the organization, which may (or may not) have consequences greater than the actual risk.

The result of this is that organizations sometimes implement specific security controls because they are required by laws, regulations, or standards—not because their risk analysis would otherwise compel them to do so.

IT Management Practices

The primary services in the IT organization typically are development, operations, and support. These primary activities require the support of a second layer of activities that together support the delivery of primary IT services to the organization. The second layer of IT management practices consists of the following:

- Personnel management
- Sourcing
- Third-party service delivery management
- Change management
- Financial management
- Quality management
- Portfolio management
- Controls management
- Security management
- Performance and capacity management

Some of these activities the IT organization undertakes itself, whereas some are usually performed by other parts of the organization. For instance, most of the personnel management functions are typically carried out by a human resources department. This is another essential reason for the existence of an organizationwide IT steering committee that is represented by members of other departments such as human resources. This enables the entire spectrum of IT management to be centrally controlled even when other departments perform some IT management functions.

Personnel Management

Personnel management encompasses many activities related to the status of employment, training, and the acceptance and management of policy. These personnel management activities ensure that the individuals who are hired into the organization are suitably vetted, trained, and equipped to perform their functions. It is important that they are provided with the organization's key policies so that their behavior and decisions will reflect the organization's needs.

Hiring

The purpose of the employee hiring process is to ensure that the organization hires persons who are qualified to perform their stated job duties and that their personal, professional, and educational histories are appropriate. The hiring process includes several activities necessary to ensure that candidates being considered are suitable.

Background Verification

Various studies suggest that 30 to 80 percent of employment candidates exaggerate their education and experience on their résumé, and some candidates commit outright fraud by providing false information about their education or prior positions. Because of this, employers need to perform their own background investigation on an employment candidate to obtain an independent assessment of the candidate's true background.

Employers should examine the following parts of a candidate's background prior to hiring:

- **Employment background:** The employer should check at least two years back, although five to seven years is needed for mid- or senior-level personnel.
- **Education background:** The employer should confirm that the candidate has earned the degrees or diplomas listed on their résumé. There are many "diploma mills," enterprises that will print a fake college diploma for a fee.
- **Military service background:** If the candidate served in any branch of the military, this must be verified to confirm whether the candidate served at all, whether they received relevant training and work experience, and whether their discharge was honorable or otherwise.
- **Professional licenses and certifications:** If a position requires that the candidate possess licenses or certifications, these need to be confirmed, including whether the candidate is in good standing with the organizations that manage those licenses and certifications.
- **Criminal background:** The employer needs to investigate whether the candidate has a criminal record. In countries with a national criminal registry, such as the National Crime Information Center (NCIC) in the United States, this is simpler than in countries that have no nationwide criminal records database. Some industrialized countries do not permit criminal background checks (believe it or not).

- **Credit background:** Where permitted by law, the employer may want to examine a candidate's credit and financial history. There are two principal reasons for this type of check: First, a good credit history indicates the candidate is responsible, while a poor credit history may be an indication of irresponsibility or poor choices (although in many cases a candidate's credit background is not entirely their own doing); second, a candidate with excessive debt and a poor credit history may be considered a risk for embezzlement, fraud, or theft.
- **Terrorist association:** Some employers want to know whether a candidate has documented ties with terrorist organizations. In the United States, an employer can request verification of whether a candidate is on one of several lists of individuals and organizations with whom U.S. citizens are prohibited from doing business. Lists are maintained by the Office of Foreign Assets Control (OFAC), by a department of the U.S. Treasury, and by the U.S. Bureau of Industry and Security.
- **References:** The employer may want to contact two or more personal and professional references—people who know the candidate and will vouch for their background, work history, and character.

In many jurisdictions, employment candidates are required to sign a consent form that will allow the employer (or a third-party agent acting on behalf of the employer) to perform the background check.

Employers also frequently research a candidate's background through word-of-mouth inquiries, Internet searches, and social media. Much useful information can be obtained that can help an employer corroborate information provided by a candidate.

Background checks are a prudent business practice to identify and reduce risk. In many industries, they are a common practice or even required by law. And in addition to performing a background check at the time of hire, many organizations perform them annually for employees in high-risk or high-value positions.

Employee Policy Manuals

Sometimes known as an employee handbook, an employee policy manual is a formal statement of the terms of employment, facts about the organization, benefits, compensation, conduct, and other policies.

Employee handbooks are often the cornerstone of corporate policy. A thorough employee handbook usually covers a wide swath of territory, including the following topics:

- **Welcome:** This welcomes a new employee into the organization, often in an upbeat letter that makes the new employee glad to have joined the organization. This may also include a brief history of the organization.
- **Policies:** These are the most important policies in the organization, which include security, privacy, code of conduct (ethics), and acceptable use of resources. In the United States and other countries, the handbook may also include antiharassment and other workplace behavior policies.

- **Compensation:** This describes when and how employees are compensated.
- **Benefits:** This describes company benefit programs.
- **Work hours:** This discusses work hours and basic expectations for when employees are expected to report to work and how many hours per week they are expected to work.
- **Dress code:** This provides a description and guidelines for required attire in the workplace.
- **Performance review:** This describes the performance review policy and program that is used periodically to evaluate each employee's performance.
- **Promotions:** This describes the criteria used by the organization to consider promotions for employees.
- **Time off:** This describes compensated and uncompensated time off, including holidays, vacation, illness, disability, bereavement, sabbaticals, military duty, and leaves of absence.
- **Security:** This discusses basic expectations on the topics of physical security and information security, as well as expectations for how employees are expected to handle confidential and sensitive information.
- **Regulation:** If the organization is subject to regulation, this may be mentioned in the employee handbook so that employees will be aware of this and conduct themselves accordingly.
- **Safety:** This discusses workplace safety, which may cover evacuation procedures, emergency procedures, permitted and prohibited items and substances (for example, weapons, alcoholic beverages, other substances and items), procedures for working with hazardous substances, and procedures for operating equipment and machinery.
- **Conduct:** This covers basic expectations for workplace conduct, both with fellow employees and with customers, vendors, business partners, and other third parties.
- **Discipline:** Organizations that have a disciplinary process usually describe its highlights in the employee handbook.

Employees are often required to sign a statement that affirms their understanding of and compliance with the employee handbook. Many organizations require that employees sign a new copy of the statement on an annual basis, even if the employee handbook has not changed. This helps to affirm for employees the importance of policies contained in the employee handbook.

Initial Access Provisioning

New employees may need access to office locations, computers, networks, and/or applications to perform their required duties. This will necessitate the provisioning of access to one or more buildings and to computer or network user accounts, as required to perform their work-related tasks.

An access-provisioning process should be used to determine which access privileges a new employee should be given. A template of job titles and access privileges should be set up in advance so that management can easily determine which access privileges any new employee will receive. Even with such a plan, each new employee's manager should formally request that these privileges be set up for new employees.

Job Descriptions

A *job description* is a formal document that describes the roles, responsibilities, and experience required. Each position in an organization, from chief executive officer to office clerk, should have a formal job description.

Job descriptions should also state that employees are required to support company policies, including but not limited to security and privacy, code of conduct, and acceptable use policies. By listing these in a job description, an employer is stating that all employees are expected to comply with these and other policies.

Employers usually are required to include several boilerplate items or statements (such as equal opportunity clauses) in job descriptions to conform to local labor and workplace safety laws.

Employee Development

Once hired into the organization, employees will require training in the organization's policies and practices so that their contributions will be effective and further the organization's goals. Regular evaluations will help employees to focus their long-term efforts on personal and the organization's goals and objectives.

Training

To be effective, employees need to receive periodic training. This includes:

- **Skills training:** Employees should learn how to use tools and equipment properly. In some cases, employees are required to receive training and prove competency before they are permitted to use some tools and equipment. Sometimes this is required by law.
- **Practices and techniques:** Employees need to understand how the organization uses its tools and equipment for its specific use.
- **Policies:** Organizations often impart information about their policies in the context of training. This helps the organization make sure that employees comprehend the material.

Performance Evaluation

Many organizations utilize a performance evaluation process to examine each employee's performance against a set of expectations and objectives. A performance evaluation program also helps to shape employees' behavior over the long term and helps them to reflect on how their efforts contribute toward the organization's overall objectives. A performance

evaluation is frequently used to determine whether (and by how much) an employee's compensation should be increased.

Career Path

In many cultures, employees believe that they can be successful if they understand how they can advance within the organization. A career path program can help employees understand what skills are required for other positions in the organization and how they can strive toward positions that they desire in the future.

Mandatory Vacations

Some organizations, particularly those that deal with high-risk or high-value activities, require mandatory vacations of one week or longer for some or all employees. This practice can accomplish three objectives:

- **Cross-training:** An absence of one week or longer will force management to cross-train other employees so that the organization is less reliant on specific individuals.
- **Audit:** A minimum absence gives the organization an opportunity to audit the absent employee's work to make sure that the employee is not involved in any undesired behavior.
- **Reduced risk:** Knowing that they will be away from their day-to-day activities for at least one or two contiguous weeks each year, employees are less apt to partake in prohibited activities that could be discovered by colleagues or auditors during their absence.

Termination

When an employee leaves an organization, these actions need to take place:

Physical access to all work areas must be immediately revoked. Depending on the sensitivity of work activities in the organization, the employee may also need to be escorted out of the work area and have their personal belongings gathered by others and delivered to the departed employee's residence.

Each of the employee's computer and network access accounts must be locked. The purpose of this action is to protect the integrity of business information by permitting only authorized employees to access it. Locking computer accounts also prevents other employees from accessing information using the former employee's credentials.

The issue of whether a former employee's account should be removed or merely disabled depends on the nature of the application or system. In some cases, the record of actions taken by employees (such as an audit log) depends on the existence of the employee's ID on the system; if a former employee's ID is removed, then those audit records may not properly reference who is associated with them.

If the organization chooses to disable rather than remove computer or network accounts for terminated employees, those accounts must be restricted in a way that positively prohibits any further access. For instance, merely changing the passwords of terminated accounts to "locked" would be considered a highly unsafe practice in the event that anyone discovers the password. If changing the account's password is the only way to disable it, then a long and highly random password must be used and then forgotten so that even the account administrator cannot use it.

In some jurisdictions, employers may be required to permit former employees to be able to access their compensation and tax records.

Transfers and Reassignments

In many organizations, employees will move between positions over time. These position changes are not always upward through a career path, but can be lateral moves from one type of work to another.

Unless an organization is very careful about its access management processes and procedures, employees who transfer and are promoted tend to accumulate access privileges. This happens because a transferring employee's old privileges are not revoked, even though those privileges are no longer needed. Over a period of years, an employee who is transferred or promoted can accumulate many excessive privileges that can indicate significant risk should the individual choose to perform functions in the applications that they are no longer officially authorized to use. This phenomenon is sometimes known as accumulation of privileges or privilege creep.

Privilege creep happens frequently in company accounting departments. An individual, for example, can move from role to role in the accounting department, all the while accumulating privileges that eventually result in the ability for that employee to defraud their employer by requesting, approving, and disbursing payments to themselves or to accomplices. Similarly, this can occur in an IT department, when an employee transfers from the operations department to the software development department (which is a common career path). Unless the IT department deliberately removes the transferring employee's prior privileges, it will end up with an employee who is a developer with access to production systems—a red flag to auditors who examine roles and responsibilities.

Contractor Management

For years, HR organizations refused to have anything to do with workers who were not employees of the organization. From the perspective of access management, this usually resulted in substandard practices for managing temporary workers, bringing increased risk to organizations. Thankfully, the tide is turning, and HR organizations are beginning to embrace the management of temporary workers. In part, this is because modern HR information systems are easily able to distinguish employees from all types of temporary

workers. Still, because of their often itinerant nature, temporary workers must be properly and accurately tracked. In the realm of access controls in sensitive environments, this represents an important risk reduction factor. Best practice would be to have both contractors and employees follow similar policies and processes, especially when they are involved in higher-risk areas of the organization.

Sourcing

Sourcing refers to the choices that organizations make when selecting the personnel who will perform functions and where those functions will be performed. Sourcing options include the following:

- **Insourced:** The organization hires employees to perform work. These workers can be full-time, part-time, or temporary.
- **Outsourced:** The organization uses contractors or consultants to perform work.
- **Hybrid:** The organization can utilize a combination of insourced and outsourced workers.

Next, the options include where personnel will perform tasks:

- **On-site:** Personnel work at the organization's worksite(s).
- **Off-site, local:** Personnel are not located on-site, but are near the organization's premises, usually in or near the same community.
- **Off-site, remote:** Personnel are in the same country, but not near the organization's premises.
- **Offshore:** Personnel are located in a different country.
- **Nearshore:** Outsourced personnel are located in a nearby country.
- **Onshore:** Outsourced personnel are located in the same country.

Organizations are often able to work out different combinations of insourced or outsourced personnel and where they perform their work. For instance, an organization can open its own office in a foreign country and hire employees to work there; this would be an example of offshore insourcing. Similarly, an organization can use contractors to perform work on-site; this is on-site outsourcing.

Insourcing

Insourcing, which is the practice of hiring employees for long-term work, is discussed earlier in this chapter in the "Personnel Management" section.

Outsourcing

Outsourcing is the practice of using contractors or consultants to perform work for the organization. An organization will decide to outsource a task, activity, or project for a wide variety of reasons:

Project duration An organization may require personnel only for a specific project, such as the development of or migration to a new application. Often, an organization will opt to use contractors or consultants when it cannot justify hiring permanent workers.

Skills An organization may require personnel with certain hard-to-find skills but may not need them on a full-time basis. Persons with certain skills may command a higher salary than the organization is willing to pay, and the organization may not have sufficient work to keep such a worker interested in permanent employment.

Variable demand Organizations may experience seasonal increases and decreases of demand for certain workers. Organizations often cannot justify hiring full-time employees for peak demand capacity, when at other times, those workers will not have enough work to keep them busy and productive. Instead, organizations will usually staff for average demand and augment staff with contractors for peak demand.

High turnover Some positions, such as IT helpdesk and call center positions, are inherently high-turnover positions that are costly to replace and train. Instead, an organization may opt to outsource some or all of the personnel in these positions.

Focus on core activities An organization may concentrate on hiring for positions related to its core purpose and to outsource functions that are considered "overhead." For instance, an organization that produces computer hardware products may elect to outsource its IT computer support department so that it can focus on its product development and support.

Financial A decision to outsource may be based primarily on financial issues. Usually, an organization seeking to reduce costs of software development and other activities will outsource and offshore these activities to service organizations located in other countries.

Complete time coverage An organization that needs to have personnel available around the clock may choose to outsource part of that function to personnel at work centers in other time zones.

An organization that chooses to hire employees only in its core service areas can outsource many of its noncore functions, including these:

- **IT helpdesk and support:** This is often a high-turnover function, as well as variable in demand, making it a good candidate for outsourcing.
- **Software development:** An organization that lacks employees with development and programming skills can elect to have contractors or consultants perform this work.

- **Software maintenance:** An organization may choose to keep its developers and analysts focused on new software development projects and to leave maintenance of existing software to contractors.
- **Customer support:** An organization may choose to outsource its telephone and online support to personnel or organizations in countries with lower labor costs.

Although outsourcing decisions appear, on the surface, to be economically motivated, some of the other reasons stated here may be even more important in some organizations. For example, the flexibility afforded by outsourcing may help to make an organization more agile, which may improve quality or increase efficiency over longer periods.

Outsourcing Benefits

Organizations that are considering outsourcing need to weigh the benefits and the costs carefully to determine whether the effort to outsource will result in measurable improvement in processing, service delivery, or finances. In the 1990s, when many organizations rushed to outsource development and support functions to operations in other countries, they did so with unrealistic short-term gains in mind and without adequately considering all of the real costs of outsourcing.

Outsourcing can bring many benefits:

- **Available skills and experience:** Organizations that may have trouble attracting persons with specialized skills often turn to outsourcing firms with highly skilled personnel who can ply their trade in a variety of client organizations.
- **Economies of scale:** Often, specialized outsourcing firms can achieve better economies of scale through discipline and mature practices that organizations are unable to achieve.
- **Objectivity:** Some functions are better done by outsiders. Personnel in an organization may have trouble being objective about some activities, such as process improvement and requirements definition. Also, auditors frequently must be employed by an outside firm to achieve sufficient objectivity and independence.
- **Reduced costs:** When outsourcing involves offshore personnel, an organization may be able to lower its operating costs and improve its competitive market position, usually through currency exchange rates and differences in the standards of living in headquarters versus offshore countries.

When an organization is making an outsourcing decision, it needs to consider these advantages together with the risks that are discussed in the next section.

Risks Associated with Outsourcing

Although outsourcing can bring many tangible and intangible benefits to an organization, it is not without certain risks and disadvantages. Naturally, when an organization employs

outsiders to perform some of its functions, it relinquishes some control. The risks of outsourcing include these:

- **Higher-than-expected costs:** Reduced costs were the main driver for offshore outsourcing in the 1990s. However, many organizations failed to anticipate all the operational realities. For instance, when outsourcing to overseas operations, IT personnel back in U.S.-based organizations may have to make many more expensive overseas trips than expected. Also, changes in international currency exchange rates can transform this year's bargain into next year's high cost.
- **Poor quality:** The outsourced work product may be lower in quality than the product created when the function was performed in-house.
- **Poor performance:** The outsourced service may not perform as expected. The capacity of networks or IT systems used by the outsourcing firm may cause processing delays or longer-than-acceptable response times.
- **Loss of control:** An organization that is accustomed to being in control of its workers may undergo a loss of control of its outsourced workers. Making small adjustments to processes and procedures may be more time-consuming or may increase costs.
- **Employee integrity and background:** It may be decidedly more difficult to determine the integrity of employees in an outsourced situation, particularly when the outsourcing is taking place offshore. Some countries, even where outsourcing is popular, lack the support of nationwide criminal background checks and other means for making a solid determination on an employee's background.
- **Loss of competitive advantage:** If the services performed by the outsourcing firm are not flexible enough to meet the organization's needs, this can result in the organization losing some of its competitive advantage. For example, suppose an organization outsources its corporate messaging (email and other messaging) to a service provider. Later, the organization wants to enhance its customer communication by integrating its service application with email. The email service provider may be unable or unwilling to provide the necessary integration, which will result in the organization losing a competitive advantage.
- **Errors and omissions:** The organization performing outsourcing services may make serious errors or may fail to perform essential tasks. For instance, an outsourcing service may suffer a data security breach that may result in the loss or disclosure of sensitive information. This can be a disastrous event when it occurs within an organization's four walls, but when it happens in an outsourced part of the business, the organization may find that the lack of control will make it difficult to take the proper steps to contain and remediate the incident. If an outsourcing firm has undergone a security breach or similar incident, it may put its own interests first and only secondarily watch out for the interests of its customers.
- **Vendor failure:** The failure of the organization to provide outsourcing services may result in increased costs and delays in service or product delivery.

- **Differing mission and goals:** An organization's employees are going to be loyal to its mission and objectives. However, the employees in an outsourced organization usually have little or no interest in the hiring organization's interests; instead, they will be loyal to the outsourcing provider's values, which may at times be in direct conflict. For example, an outsourcing organization may place emphasis on maximizing billable hours, while the hiring organization emphasizes efficiency. These two objectives conflict with each other.
- **Difficult recourse:** If an organization is dissatisfied with the performance or quality of its outsourced operation, contract provisions may not sufficiently facilitate any remedy. If the outsourced operation is in a foreign country, applying remediation in the court system may also be futile.
- **Lowered employee morale:** If an organization chooses to outsource work and lays off some full-time workers, employees who remain may be upset because some of their colleagues have lost their jobs as a result of the outsourcing. Further, remaining employees may fear that their own jobs may soon be outsourced or eliminated. They may also believe that their organization is more interested in saving money than in taking care of its employees. Personnel who have lost their jobs may vent their anger at the organization through a variety of harmful actions that can threaten assets or other workers.
- **Audit and compliance:** An organization that outsources a part of its operation that is in scope for applicable laws and regulations may find it more challenging to perform audits and achieve compliance. Audit costs may rise, as auditors need to visit the outsourced work centers. Requiring the outsourced organization to make changes to achieve compliance may be difficult or expensive.
- **Applicable laws:** Laws, regulations, and standards in headquarters and offshore countries may impose requirements on the protection of information that can complicate business operations or enterprise architectures.
- **Cross-border data transfer:** Governments around the world are paying attention to the flow of data, particularly the sensitive data of their citizens. Many countries have passed laws that attempt to exert control over data about their citizens when it is transferred out of their jurisdictions.
- **Time zone differences:** Communications will suffer when an organization outsources some of its operations to offshore organizations that are several time zones distant. It will be more difficult to schedule telephone conferences if there is very little overlap between work hours in each time zone. It will take more time to communicate important issues and to make changes.
- **Language and cultural differences:** When outsourcing crosses language and cultural barriers, it can result in less than optimal communication and results. The outsourcing customer will express its needs through its own language and culture, and the outsourcing provider will hear those needs through its own language and culture. Both sides may be thinking or saying, "They don't understand what we want" and "We don't understand what they want." This can result in unexpected differences in work produced by

the outsourcing firm. Delays in project completion or delivery of goods and services can occur as a result.

- **Political conditions:** When offshoring labor and when using foreign workers with work visas, changes in political conditions can result in restrictions of the use of foreign workers, wherever they are working. For example, restrictions on certain types of work visas for foreign workers have forced some organizations to change their strategies for attracting offshore talent.

Some of the risks associated with outsourcing are intangible or may lie outside the bounds of legal remedies. For instance, language and time zone differences can introduce delays in communication, adding friction to the business relationship in a way that may not be easily measurable.

Mitigating Outsourcing Risk

The only means of exchange between an outsourcing provider and its customer organization are money and reputation. In other words, the only leverage that an organization has against its outsourcing provider is the withholding of payment and communicating the quality (or lack thereof) of the provider's services to other organizations. This is especially true if the outsourcing crosses national boundaries. Therefore, an organization that is considering outsourcing must carefully consider how it will enforce contract terms so that it receives the goods and services that it is expecting.

Many of the risks of outsourcing can be remedied through contract provisions. Here are some of the remedies:

- **Service level agreement (SLA):** The contract should provide details for every avenue of work performance and communication, including escalations and problem management.
- **Quality:** Depending on the product or service, this may translate into an error or defect rate, a customer satisfaction rate, or system performance.
- **Security policy and controls:** Whether the outsourcing firm is safeguarding the organization's intellectual property, keeping business secrets, or protecting information about its employees or customers, the contract should spell out the details of the security controls that it expects the outsourcing firm to maintain. The organization should also require periodic third-party audits and the results of those audits. The contract should contain a "right to audit" clause that allows the outsourcing organization to examine the work premises, records, and workpapers on demand.
- **Business continuity:** The contract should require the outsourcing firm to have reasonable measures and safeguards in place to ensure resilience of operations and the ability to continue operations with minimum disruption in the event of a disaster.
- **Employee integrity:** The contract should define how the outsourcing firm will vet its employees' backgrounds so that it is not inadvertently hiring individuals with a criminal history and so employees' claimed education and work experience are proven genuine.

- **Ownership of intellectual property:** If the outsourcing firm is producing software or other designs, the contract must define ownership of those work products and whether the outsourcing firm may reuse any of those work products for other engagements.
- **Roles and responsibilities:** The contract should specify in detail the roles and responsibilities of each party so that each will know what is expected of them.
- **Schedule:** The contract must specify when and how many items of work product should be produced.
- **Regulation:** The contract should require both parties to conform to all applicable laws and regulations, including but not limited to intellectual property, data protection, and workplace safety.
- **Warranty:** The contract should specify terms of warranty so that there can be no ambiguity regarding the quality of goods or services performed.
- **Dispute and resolution:** The contract should contain provisions that define the process for handling and resolving disputes.
- **Payment:** The contract should specify how and when the outsourcing provider will be paid. Compensation should be tied not only to the quantity but also to the quality of work performed. The contract should include incentive provisions for additional payment when specific schedule, quantity, or quality targets are exceeded. The contract should also contain financial penalties that are enacted when SLA, quality, security, audit, or schedule targets are missed.

The terms of an outsourcing contract should adequately reward the outsourcing firm for a job well done, which should include the prospect of earning additional contracts as well as referrals that will help it to earn outsourcing contracts from other customers.

Outsourcing Governance

You cannot outsource accountability. Outsourcing is a convenient way to transfer some operations to an external organization, thereby allowing the outsourcing organization to be more agile and allowing the outsourcing organization to improve focus on core competencies. Although senior managers can transfer these activities to external organizations and even specify rewards for good performance and penalties for substandard performance, those senior managers are still ultimately accountable for the delivery of these services, whether they are outsourced or performed by internal staff.

In the context of outsourcing, the role of governance must be expanded to include the aggregation of activities that control the work performed by external organizations. Governance activities may include the following:

Contracts The overall business relationship between the organization and its service providers should be defined in detailed legal agreements. The terms of legal agreements should define the work to be done (in general), the expectations of all parties, service levels, quality, the terms of compensation, and remedies in case expectations fail to be met. Appropriate levels of management must approve the content in contracts.

Work Orders Sometimes called statements of work (SOWs), work orders describe in greater detail the work that is to be performed. While contracts are seldom changed, work orders operate in short-term intervals and are specific to currently delivered goods or services. Like contracts themselves, work orders should include precise statements regarding work output, timeliness, quality, and remedies.

Service Level Agreements These documents specify service levels in terms of the quantity of work, quality, timeliness, and remedies for shortfalls in quality or quantity.

Change Management A formal method is needed so that changes in delivery specifications can be formally controlled.

Security If the service provider has access to the organization's records or other intellectual property, the organization will require that specific security controls be in place. In higher-risk situations, the organization will want to validate periodically that the service provider's security controls are effective.

Quality Minimum standards for quality should be expressed in detail so that both service provider and customer have a common understanding of the expected quality of work to be performed.

Metrics Often, the outsourcing organization will want to actively measure various aspects of the outsourced activity to gain short-term visibility into work output as well as the ability to understand long-term trends.

Audits The outsourcing organization may require that audits of the outsourced work be performed. These audits may be performed by a competent third party, by an independent security consulting firm, or by the customer. Often, an outsourcing organization will negotiate a "right to audit" clause in the contract but will exercise this only if the organization encounters irregularities or issues related to the work performed.

Depending on the nature of specific outsourcing arrangements, the preceding activities may be combined or performed separately.

Benchmarking

Benchmarking measures a process to compare its performance and quality against the same process in other organizations. Its purpose is to discover opportunities for improvement that may result in lower costs, fewer resources, and higher quality.

In the context of outsourcing, benchmarking can be used to measure the performance of an outsourced process against the same process performed by other outsourcing firms, as well as to compare it with the same process performed internally by other organizations. The objective is the same: to learn whether a particular outsourcing solution is performing effectively and efficiently.

Third-Party Service Delivery Management

Service delivery management is the institution of controls and metrics to ensure that services are performed properly and with a minimum of incidents and defects. When activities are

transferred to a service provider, service delivery management has some added dimensions and considerations.

When service delivery management is used to manage an external service provider, the service provider is usually required to maintain detailed measurements of its work output. The organization utilizing an external service provider also needs to maintain detailed records of work received, and it should perform its own defect management controls to ensure that the work performed by the service provider meets quality standards. Problems and incidents encountered by the organization should be documented and transmitted to the service provider to improve quality.

These activities should be included in the SLA or in the contract to ensure that the customer will be able to impose financial penalties or other types of leveraging on to the service provider to improve quality while maintaining minimum work output.

Service delivery standards related to IT service management are defined in the international standard ISO/IEC 20000:2018. Relevant controls from this standard can be used to impose a standard method for managing service delivery by the service provider.

Third-party risk management (TPRM) is a similar activity with regard to the management of service providers. TPRM is discussed in detail in Chapter 7, "Information Security Management."

SaaS, IaaS, and PaaS Considerations

Organizations such as SaaS (software-as-a-service), IaaS (infrastructure-as-a-service), and PaaS (platform-as-a-service) provide cloud-based application or computing resources to clients that cannot justify building their own.

SaaS is an arrangement in which an organization obtains a software application for use by its employees, where the software application is hosted by the software provider as opposed to the customer organization. IaaS is an arrangement in which an organization rents IT infrastructure from a service provider. PaaS is a service that enables organizations to deploy applications without having to deal with underlying infrastructure such as servers and database management systems.

The primary advantages of using SaaS, IaaS, and PaaS as opposed to self-hosting are as follows:

- **Capital savings:** The SaaS/IaaS/PaaS provider makes its software, infrastructure, or platform resources available to its customers on its own servers, thereby eliminating a customers' need to purchase dedicated hardware and software.
- **Labor savings:** The SaaS/IaaS/PaaS provider performs many administrative functions, including typical administrative tasks such as applying software or operating system patches, managing performance and capacity, upgrading software, and troubleshooting.

In addition to the advantages outlined here, the use of SaaS/IaaS/PaaS providers can also assist a company in risk management, as discussed previously, by transferring key risks to the service provider.

An organization that is considering an SaaS, an IaaS, or a PaaS provider for one of its environments will need to ensure that the provider has adequate controls in place to protect the organization's data. Specifically,

an organization needs to understand the security responsibility model thoroughly to determine which controls are performed by the service provider and which have to be implemented by the organization. Further, the provider should have controls in place that will prevent one customer from being able to view the data associated with a different customer.

An organization can consider the SaaS/IaaS/PaaS provider to be similar to other service providers. Generally, methods used to determine the integrity and quality of the SaaS/IaaS/PaaS provider would be the same as those used with other service providers.

Business Process-as-a-Service

As the cybersecurity skills shortage widens, service organizations are developing numerous business process-as-a-service offerings to help businesses continue critical security processes. Examples of new service offerings include identity-as-a-service, vulnerability management-as-a-service, and patch management-as-a-service. One of the first "as-a-service" offerings was security event monitoring, which is still popular.

Change Management

Change management is a business process that is used to control changes made to an IT environment. A formal change management process consists of several steps that are carried out for each change:

1. Request.
2. Review.
3. Approve (or deny).
4. Perform.
5. Verify.
6. Back out (when verification of a successful change fails).

Each step in change management includes recordkeeping. Change management is covered in detail in Chapter 3, "IT Life Cycle Management."

Financial Management

Sound financial management is critical in any organization. Because IT is a cost-intensive activity, it is imperative that the organization be well managed, with short-term and long-term budget planning, and that it track actual spending.

One area where senior management needs to make strategic financial decisions in IT is the manner in which it acquires software applications. At the steering committee level, IT organizations carefully need to weigh "make versus buy" with their primary applications. This typically falls into three alternatives:

- **Develop the application:** The organization develops the application using in-house or contracted software developers, designers, and analysts.
- **Purchase the application:** The organization licenses the application from a software vendor and installs it on servers that it leases or purchases.
- **Rent the application:** This generally refers to the cloud computing or SaaS model, whereby the cloud/application service provider hosts the application on its own premises (or in an Internet data center) and the organization using the software pays either a fixed fee or an on-demand fee. The purchasing organization will have no capital cost for servers and little or no development cost (except, possibly, for interfaces to other applications).

The choice that an organization makes is not just about the finances, but is also concerned with the degree of control that the organization requires.

IT financial management is about not only applications, but also the other services that an IT organization provides. Other functions such as service desk, PC build and support, email, and network services can likewise be insourced or outsourced, each with financial and other implications.

Many larger organizations employ a "chargeback" feature for the delivery of IT services. In this method, an IT organization charges (usually through budget transfers but occasionally through real funds) for the services that it provides. The advantage to chargeback is that the customers of the IT organization are required to budget for IT services and are less likely to make frivolous requests of IT, since every activity has a cost associated with it. Chargeback may also force an IT organization to be more competitive, as chargeback may invite IT customers to acquire services from outside organizations and not from the internal IT organization. Chargeback can thus be viewed as outsourcing to the internal IT organization.

Quality Management

Quality management refers to the methods by which business processes are controlled, monitored, and managed to bring about continuous improvement. The scope of a quality management system in an IT organization may cover any or all of the following activities:

- Software development
- Software acquisition
- Service desk

- IT operations
- Security

The components that are required to build and operate a quality management system are as follows:

- **Documented processes:** Each process that is part of a quality management system must be fully documented. This means that all of the tasks, notifications, records, and data flows must be fully described in formal process documents that are themselves controlled.
- **Key measurements:** Each process under quality management must have some key measurement points so that management will be able to understand the frequency and effort expended for the process. Measurement goes beyond simply tallying and must include methods for recognizing, classifying, and measuring incidents, events, problems, and defects.
- **Management review of key measurements:** Key measurements need to be regularly analyzed and included in status reports that provide meaningful information to various levels of management. This enables management to understand how key processes are performing and whether they are meeting management's expectations.
- **Audits:** Processes in a quality management system should be periodically measured by internal or external auditors to ensure that they are being operated properly. These auditors need to be sufficiently independent of the processes and of management itself so that they can objectively evaluate processes.
- **Process changes:** When key measurements suggest that changes to a process are needed, a business or process analyst will make changes to the design of a process. Examples of process changes include the addition of data fields in a change request process, the addition of security requirements to the software development process, or a new method for communicating passwords to the users of newly created user accounts.

An organization should document and measure its quality management processes, just as it does with all of the processes under its observation and control. This will help to confirm whether the quality management system itself is effective.

ISO/IEC 9000

Established in the 1980s, the ISO/IEC 9000 family of standards remains the gold standard for quality management systems.

Organizations that implement the ISO/IEC 9001:2015 standard can voluntarily undergo regular external audits by an accredited firm to earn an ISO/IEC 9001:2015 certification. More than one million ISO/IEC 9001 certificates have been issued to organizations around the world since 1987.

ISO/IEC 9000 began as a manufacturing product quality standard. While many manufacturing firms are certified to ISO/IEC 9000, the standard is growing in popularity among service providers and software development organizations.

ISO/IEC 20000

Many IT organizations have adopted ITIL IT service management processes as a standard framework for IT processes. Organizations that desire a certification can be evaluated by an accredited external audit firm to confirm that they conform to the ISO/IEC 20000 IT Service Management standard. ISO/IEC 20000 supersedes the earlier BS 15000 standard.

The ITIL 4 framework consists of 34 management practices in three categories:

- General Management Practices
- Service Management Practices
- Technical Management Practices

The ITIL 4 framework consists of four dimensions:

- Organization and People
- Value Streams and Processes
- Partners and Suppliers
- Information and Technology

ITIL's management practices constitute an effective framework for IT's primary function: delivering valuable services to enable key organizational processes.

Portfolio Management

Portfolio management refers to the systematic management of IT projects, investments, and activities. The purpose of portfolio management is to measure the value derived from IT projects, investments, and activities and to make adjustments periodically to maximize that value for the organization.

The principles of IT portfolio management are similar to those of financial investment portfolio management. All of the activities in IT are treated like investments, with a careful look at the value they bring to the organization.

Mature organizations that practice IT portfolio management typically develop three portfolios:

- Project portfolio
- Infrastructure portfolio
- Application portfolio

The items in these portfolios are measured, examined, and scrutinized for their continuing contribution to, and alignment with, the organization's mission and main objectives. Management can make periodic adjustments to the level of resources associated with IT projects and activities to maximize value to the organization.

Controls Management

IT organizations employ controls to ensure specific outcomes within business processes, IT systems, and personnel. Better organizations adopt one of several standard frameworks of controls and then periodically assess risk and control performance, resulting in changes to controls as well as the addition or removal of controls.

Controls are generally enacted as a result of one or more of the following:

- **Policies:** Controls can be established to ensure compliance to a policy and to measure a policy's effectiveness.
- **Regulations:** Organizations often establish controls to ensure compliance with regulations.
- **Requirements:** Legal or operational requirements, such as terms and conditions in contracts with customers or suppliers, compel an organization to enact controls to ensure compliance.
- **Risks:** An internal or external risk assessment may compel an organization to enact controls to reduce risks to acceptable levels.
- **Incidents:** A compelling incident or event may prompt an organization to enact controls to prevent similar incidents from recurring.

It is not enough for organizations to develop and implement controls. Organizations need to examine controls periodically to determine whether they are operating properly and ensuring their intended outcomes. The entire discipline of internal and external audit is brought to bear on the subject of control examination and effectiveness. The process and practice of audits is explored in detail in Chapter 9, "Conducting a Professional Audit."

Well-known control frameworks include:

- **COBIT 2019:** Developed by ISACA, COBIT 2019 is a general-purpose IT controls framework.
- **NIST 800-53:** Developed by the National Institute of Standards and Technology (NIST), NIST 800-53 is a comprehensive set of security and privacy controls for information systems. This framework has been adopted by many government and nongovernment organizations.
- **NIST Cybersecurity Framework (CSF) 2.0:** This framework organizes controls into six functions: Govern, Identify, Protect, Detect, Respond, and Recover. CSF also serves as a guide for organizations to determine their security maturity.
- **ISO/IEC 20000:** This is the international standard with its roots in the ITIL, the framework of IT service management.
- **ISO/IEC 27002:** This is the international standard framework of IT security controls, and it is widely adopted worldwide.
- **PCI DSS 4.0 (Payment Card Industry Data Security Standard):** This is the IT security controls framework required for systems and networks that store, process, or transmit credit and debit card data.

- **HIPAA (Health Insurance Portability and Accountability Act) Security Rule:** This is the framework of controls required for organizations that store, process, or transmit electronic patient health information (ePHI).
- **Center for Internet Security (CIS) Critical Security Controls:** Originally developed by the SANS Institute, CIS Critical Security Controls consist of 18 controls. As an integral part of information security and IT audit, these controls are discussed throughout this book.

Security Management

Security management refers to several key activities that work together to identify risks and risk treatment for the organization's assets. In most organizations these activities include:

Security Governance This is the practice of setting organizational security policy and then taking steps to ensure that the policy is followed. Security governance also is involved with the management and continuous improvement of other key security activities discussed in this section.

Risk Assessment This is the practice of identifying key assets in use by the organization and identifying vulnerabilities in, and threats against, each asset. This is followed by the development of risk treatment strategies that attempt to mitigate, transfer, avoid, or accept identified risks.

Incident Management This practice is concerned with the planned response to security incidents when they occur in the organization. An incident is defined as a violation of security policy; such an incident may be minor (such as a user choosing an easily guessed password) or major (such as a hacking attack and theft of sensitive information). Aspects of incident management include computer forensics (the preservation of evidence that could be used in later legal action) and the involvement of regulatory authorities and law enforcement.

Vulnerability Management This is the practice of proactively identifying vulnerabilities in IT systems, as well as in business processes, that could be exploited to the detriment of the organization. Activities that take place in vulnerability management include security scanning, vulnerability assessment, code review, patch management, and reviewing threat intelligence and risk advisories issued by software vendors and security organizations.

Identity and Access Management These practices are used to control which persons and groups may have access to which applications, assets, systems, workplaces, and functions. Identity management is the activity of managing the identity and access history of each employee, contractor, temporary worker, supplier worker, and, optionally, customer. These records are then used as the basis for controlling which workplaces, applications, IT systems, and business functions each person is permitted to use.

Compliance Management Security management should be responsible for knowing which laws, regulations, standards, requirements, and legal contracts the organization is required to comply with. Verification of compliance may involve internal or external audits and other activities to confirm that the organization is in compliance with all of these legal and other requirements.

Third-Party Risk Management This is the practice of identifying and managing risks associated with third-party organizations that store, process, or transmit sensitive information on behalf of the organization. Activities include up-front due diligence and periodic assessment of critical control effectiveness and overall business risk.

Business Continuity and Disaster Recovery Planning These practices enable the organization to develop response plans in the event that a disaster should occur that would otherwise threaten the ongoing viability of the organization. Business continuity and disaster recovery planning is covered in detail later in this chapter.

Control frameworks for security management include:

- **ISO/IEC 27001 requirements:** The first half of the ISO/IEC 27001 standard contains a set of requirements that describe a scalable and flexible information security management system (ISMS) that is based on a life cycle of risk assessment, controls examination, and controls development, with an overarching theme of executive oversight and control.

Performance and Capacity Management

Performance optimization is concerned with the continual improvement of IT processes and systems. This set of activities is concerned not only with financial efficiency, but also with the time and resources required to perform common IT functions. The primary objective of IT performance optimization is to ensure that the organization is getting the maximum benefit from IT services for the lowest possible expenditure of resources.

An organization that measures process performance is more apt to recognize opportunities for making improvements to business processes. Organizations that reach a level of process maturity that includes measurement and feedback will be able to adopt a culture of continuous improvement. Then management can track improvement opportunities and assign resources accordingly.

Performance optimization is considered a rather mature approach to the management of IT processes and systems. It requires mature processes with key controls and measurement points, and it is one of the natural results of effective quality management. An organization that is not already monitoring and managing its processes is probably not ready to undertake performance optimization. See the earlier section, "Quality Management," for more information on this perspective.

Performance optimization is a complicated undertaking, because IT systems and processes usually change frequently over time; it can be difficult to attribute specific changes in systems or processes to changes in performance metrics.

Maturity models such as Capability Maturity Model Integration (CMMI) can be used to determine the level of an organization's processes. CMMI focuses on whether an organization's processes have a level of maturity associated with measurement and continuous improvement.

The COBIT 2019 framework also contains facilities to identify and measure KPIs, with the aim of enabling continuous improvement to processes and technology. The COBIT framework contains 40 governance and management objectives, along with the means for any individual organization to determine how much (and what kind of) control is appropriate for the organization, based on its business objectives and how IT supports them.

A typical organization will not have the same level of maturity across all of its departments and processes. Instead, some processes and departments will be more mature than others, often by a wide variance.

Benchmarking

An organization may decide to benchmark its key processes. Benchmarking is a process of performing a detailed comparison of a business process (or system, or almost any other aspect of an organization) with the same process in other organizations. This will help an organization better understand how similar organizations are solving similar business problems, which could lead the organization to enact process improvements on its own.

In the past, it was common for organizations to benchmark the overall cost of information technology or information security. Today, however, IT and security costs are more ambiguous, particularly considering the trend of outsourcing business and IT services to third parties. Hence, it has become more useful to benchmark process maturity or risk appetite as a way of comparing an organization to its peers.

Organization Structure and Responsibilities

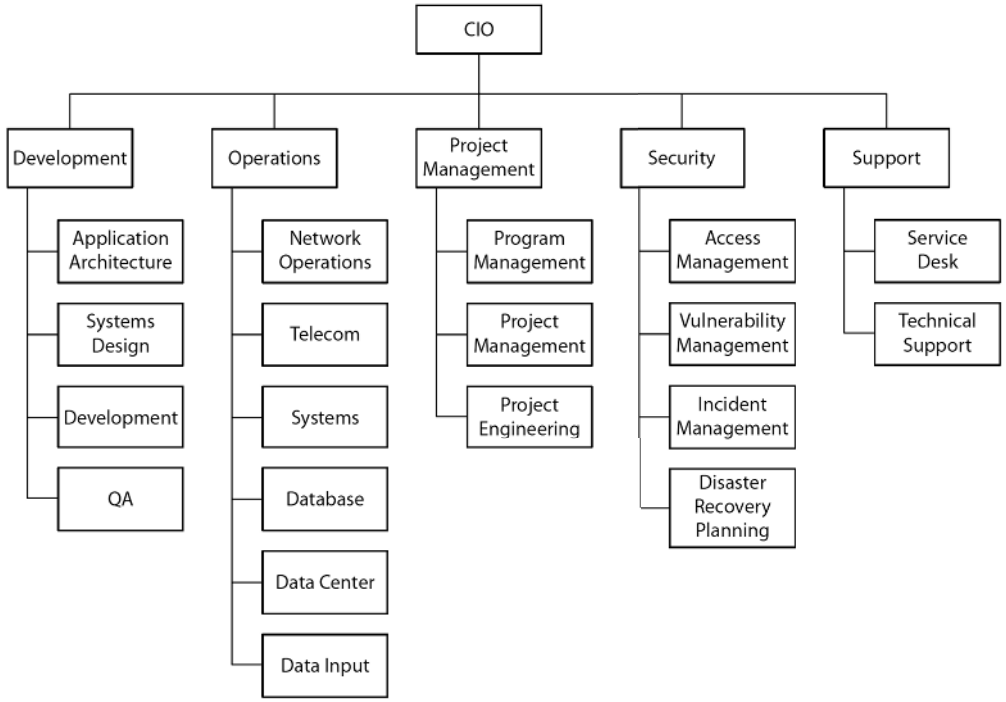
Organizations require structure to distribute responsibility to groups of people with specific skills and knowledge. The structure of an organization is depicted in an organization chart (org chart). Figure 1.5 shows a typical IT organization chart.

Organizing and maintaining an organization structure requires that many factors be considered. In most organizations, the org chart is a living structure that changes from time to time, based on several conditions, including the following:

- **Short- and long-term objectives:** Organizations sometimes move departments from one executive to another so that departments that were once far from each other (in terms of the org chart structure) will be near each other. This provides new opportunities for developing synergies and partnerships that did not exist before the reorganization. These organizational changes are usually performed to help an organization meet

new objectives that were less important before and that require new partnerships and teamwork.

FIGURE 1.5 Typical IT organization chart



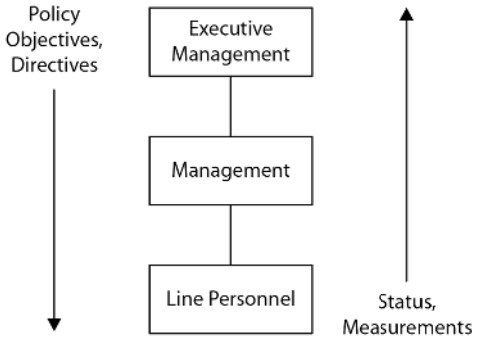
- **Market conditions:** Changes in market positions can cause an organization to realign its internal structure to strengthen itself. For example, if a competitor lowers its prices based on a new sourcing strategy, an organization may need to respond by changing its organizational structure to put experienced executives in charge of specific activities.
- **Regulations:** New laws, regulations, or standards may induce an organization to change its organizational structure. For instance, an organization that becomes highly regulated may elect to move its security and compliance group away from IT and place it under the legal department, since compliance has much more to do with legal compliance than industry standards.
- **Attrition and available talent:** When someone leaves the organization or moves to another position within the organization, particularly in positions of leadership, a space opens in the org chart that often cannot be filled right away. Instead, senior management will temporarily change the structure of the organization by moving the leaderless department under the control of someone else. Often, the decisions of how to change the organization will depend on the talent and experience of existing leaders, in addition

to each leader's workload and other factors. For example, if the director of IT program management leaves the organization, the existing department could temporarily be placed under the IT operations department, in this case because the director of IT operations used to run IT program management. Senior management can see how that arrangement works out and later decide whether to replace the director of IT program management position or do something else.

Many organizations use formal succession planning as a way of preparing for unexpected changes in the organization, especially terminations and resignations. A succession plan helps the organization temporarily fill an absent position until a long-term replacement can be found.

This structure serves as a top-down and bottom-up conduit of communication. Figure 1.6 depicts the communication and control that an organization provides.

FIGURE 1.6 Communication and control flow upward and downward in an organization.



Roles and Responsibilities

The topic of roles and responsibilities is multidimensional; it encompasses positions and relationships on the organization chart, it defines specific job titles and duties, and it denotes generic expectations and responsibilities regarding the use and protection of assets.

Individual Roles and Responsibilities

Several roles and responsibilities fall upon all individuals throughout the organization:

- **Board of directors:** The organization's governing body is legally responsible for overseeing the organization's activities, as well as the selection, support, and review of the chief executive. In private industry, boards are composed of the organization's senior

executives as well as executives from other firms, including firms with a significant investment in the organization. In government, directors are often elected. Increasingly, directors are held to a higher standard of personal responsibility regarding the management and outcomes of the organizations they lead.

- **Executive management:** The most senior managers and executives in an organization are responsible for developing the organization's mission, objectives, and goals, as well as policy. Executives are responsible for enacting security policy, which defines (among other things) the protection of assets.
- **Owner:** An owner is an individual (usually but not necessarily a manager) who is the designated owner-steward of an asset. Depending on the organization's security policy, an owner may be responsible for the maintenance and integrity of the asset, as well as for deciding who is permitted to access the asset. If the asset is information, the owner may be responsible for determining who can access and make changes to the information.
- **Manager:** Managers are, in the general sense, responsible for understanding the organization's policies and procedures and making them available to their staff members. They should also, to some extent, be responsible for their staff members' behavior.
- **User:** Users are individuals (at any level of the organization) who use assets in the performance of their job duties. Each user is responsible for how they use the asset, and each user does not permit others to access the asset in the user's name. Users are responsible for performing their duties lawfully and for conforming to organization policies.

These generic roles and responsibilities should apply across the org chart to include every person in the organization. Persons in these roles may be full-time or part-time employees, or they may be temporary workers such as contractors and consultants.

The roles and responsibilities of executives, owners, managers, and users should be formally defined in an organization's security policy.

Job Titles and Job Descriptions

A job title is a label that is assigned to a job description. A job title denotes a position in the organization that has a given set of responsibilities and that requires a certain level and focus of education and prior experience. A job description is a list of those responsibilities and required education and experience.

Exam Tip

The CISA exam may present questions that address proper procedures for the audit of a specified job title. When considering your response, think about the job role assigned to the specific title rather than focusing on the title itself. Questions that address job titles are intended to examine your understanding of their related roles—an example being the network management role associated with the network engineer title.

An organization with a program of career advancement may have a set of career paths or career ladders that model how employees may advance. For each job title, a career path will show the possible avenues of advancement to other job titles and the experience required to reach those job titles.

Job titles in IT have matured and are quite consistent across organizations. This consistency helps organizations in several ways:

- **Recruiting:** When the organization needs to find someone to fill an open position, the use of standard job titles will help prospective candidates more easily find positions that match their criteria.
- **Compensation baselining:** Because of the chronic shortage of talented IT workers, organizations are forced to be more competitive when trying to attract new workers. To remain competitive, many organizations periodically undertake a regional compensation analysis to understand the levels of compensation paid to IT workers in other organizations. The use of standard job titles makes the task of comparing compensation far easier.
- **Career advancement:** When an organization uses job titles that are consistent in the industry, IT workers have a better understanding of the functions of positions within their own organizations and can more easily plan how they can advance.

The remainder of this section includes many IT job titles with a short description (not a full job description by any measure) of the function of that position.

Virtually all organizations also include titles that denote the level of experience, leadership, or span of control in an organization. These titles may include executive vice president, senior vice president, vice president, executive director, senior director, director, general manager, senior manager, manager, and supervisor. Larger organizations will use more of these and possibly additional titles such as regional manager, district manager, group manager, or area manager.

Executive Management

Executive managers are the chief leaders and policymakers in an organization. They set objectives and work directly with the organization's most senior management to help make decisions affecting the future strategy of the organization:

- **CIO (chief information officer):** This is the title of the topmost leader in a larger IT organization.
- **CTO (chief technical officer):** This position is usually responsible for an organization's overall technology strategy. Depending on the purpose of the organization, this position may be separate from IT.
- **CRO (chief risk officer):** This position is responsible for all aspects of risk, including information risk, business risk, compliance risk, and market risk. This role is separate from IT.
- **CSO (chief security officer):** This position is responsible for all aspects of security, including information security, physical security, and possibly executive protection (protecting the safety of senior executives). This role is separate from IT.

- **CISO (chief information security officer):** This position is responsible for all aspects of information-related security. This usually includes incident management, disaster recovery, vulnerability management, and compliance. This role is usually separate from IT.
- **CIRO (chief information risk officer):** This position is responsible for all aspects of information-related risk management. The CIRO position symbolizes the risk management emphasis of information security.
- **CPO (chief privacy officer):** This position is responsible for the protection and use of personal information. This position is present in organizations that collect and store sensitive information for large numbers of persons.
- **CCO (chief compliance officer):** This position has broad responsibility for compliance, including information protection and privacy. Organizations under a heavy regulatory burden employ a CCO, who is responsible for compliance across a broad spectrum of regulations and requirements.
- **CAIO (chief artificial intelligence officer):** This position is responsible for the strategy, implementation, and governance of artificial intelligence technologies and systems within the organization. The CAIO ensures that AI initiatives align with business goals and regulatory requirements.

Software Development

Those in positions in software development are involved in the design, development, and testing of software applications:

- **Systems architect:** This position is usually responsible for the overall information systems architecture in the organization. This may or may not include overall data architecture as well as interfaces to external organizations.
- **Systems analyst:** A systems analyst is involved with the design of applications, including changes in an application's original design. This position may develop technical requirements, program design, and software test plans. In cases where organizations license applications developed by other companies, systems analysts design interfaces to other applications.
- **Software engineer/developer:** This position develops application software. Depending on the level of experience, persons in this position may also design programs or applications. In organizations that utilize purchased application software, developers often create custom interfaces, application customizations, and custom reports.
- **Software tester:** This position tests changes in programs made by software engineers/developers.

Data Management

Those in positions in data management are responsible for developing and implementing database designs and for maintaining databases:

- **Data manager:** This position is responsible for data architecture and data management in larger organizations.

- **Data scientist:** This position is responsible for employing scientific methods to gain knowledge from data.
- **Big data architect:** This position develops data models and data analytics for large, complex datasets.
- **Database architect:** This position develops logical and physical designs of data models for applications. With sufficient experience, this person may also design an organization's overall data architecture.
- **Database administrator (DBA):** This position builds and maintains databases designed by the database architect and those databases that are included as a part of purchased applications. The DBA monitors databases, tunes them for performance and efficiency, and troubleshoots problems.
- **Database analyst:** This position performs tasks that are junior to the database administrator, carrying out routine data maintenance and monitoring tasks.

Exam Tip

The roles of data manager, data scientist, big data architect, database architect, database administrator, and database analyst are distinct from the data owner. The former are IT department roles for managing data technology, whereas the data owner role governs the business use of data in information systems.

Network Management

Those in positions in network management are responsible for designing, building, monitoring, and maintaining voice and data communications networks, including connections to outside business partners and the Internet:

- **Network architect:** This position designs data and voice networks and designs changes and upgrades to networks as needed to meet new organization objectives.
- **Network engineer:** This position implements, configures, and maintains network devices such as routers, switches, firewalls, and gateways.
- **Network administrator:** This position performs routine tasks in the network such as making configuration changes and monitoring event logs.
- **Telecom engineer:** This position works with telecommunications technologies such as telecom services, data circuits, phone systems, conferencing systems, and voicemail systems.

Systems Management

Those in positions in systems management are responsible for architecture, design, building, and maintenance of servers and operating systems. This may include desktop operating systems as well.

- **Systems architect:** This position is responsible for the overall architecture of systems (usually servers), which includes both the internal architecture of a system and the relationship between systems. This position is usually also responsible for the design of services such as authentication, email, and time synchronization.
- **Systems engineer:** This position is responsible for designing, building, and maintaining servers and server operating systems.
- **Storage engineer:** This position is responsible for designing, building, and maintaining storage subsystems.
- **Systems administrator:** This position is responsible for performing maintenance and configuration operations on systems.

Operations

Those in positions in operations are responsible for day-to-day operational tasks that may include networks, servers, databases, and applications:

- **Operations manager:** This position is responsible for overall operations that are carried out by others. Responsibilities include establishing operations shift schedules, ensuring compliance with operational policies, and managing operational budgets.
- **Operations analyst:** This position may be responsible for the development of operational procedures; examining the health of networks, systems, and databases; setting and monitoring the operations schedule; and maintaining operations records.
- **Controls analyst:** This position is responsible for monitoring batch jobs, data entry work, and other tasks to make sure that they are operating correctly.
- **Systems operator:** This position is responsible for monitoring systems and networks, performing backup tasks, running batch jobs, printing reports, and other operational tasks.
- **Data entry:** This position is responsible for keying batches of data from hard copy or other sources.
- **Media manager:** This position is responsible for maintaining and tracking the use and whereabouts of backup tapes and other media.

Security Operations

Those in positions in security operations are responsible for designing, building, and monitoring security systems and security controls to ensure the confidentiality, integrity, and availability of information systems:

- **Security architect:** This position is responsible for the design of security controls and systems such as authentication, audit logging, intrusion detection systems (IDSs), IPSs, and firewalls.
- **Security engineer:** This position is responsible for building and maintaining security services and systems that are designed by the security architect.

- **Security analyst:** This position is responsible for examining logs from firewalls, intrusion detection and prevention systems, and audit logs from systems and applications. This position may also be responsible for issuing security advisories to others in IT.
- **Access administrator:** This position is responsible for accepting approved requests for user access management changes and performing the necessary changes at the network, system, database, or application level. Often, this position is carried out by personnel in network and systems management functions; only in larger organizations is user account management performed in the security or even in a separate user access department.
- **Security auditor:** This position is responsible for performing internal audits of IT controls to ensure that they are being operated properly.

The security auditor position needs to be carefully placed in the organization so that persons in this role can be objective and independent from the departments they audit. In U.S. public companies and other organizations, the internal audit function often reports directly to the audit committee of the board of directors.

Service Desk

Those in positions at the service desk are responsible for providing frontline support services to IT and IT's customers:

- **Service desk manager:** This position serves as a liaison between end users and the IT service desk department.
- **Helpdesk analyst:** This position is responsible for providing frontline user support services to personnel in the organization.
- **Technical support analyst:** This position is responsible for providing technical support services to other IT personnel and perhaps to IT customers.

Quality Assurance

Those in positions in quality assurance are responsible for developing IT processes and standards and for measuring IT systems and processes to confirm their accuracy:

- **QA manager:** This position is responsible for facilitating quality improvement activities throughout the IT organization.
- **QC manager:** This position is responsible for quality control through the testing of IT systems and applications to confirm whether they are free of defects.

Other Roles

Other roles in IT organizations include:

- **Vendor manager:** This position is responsible for maintaining business relationships with external vendors, measuring their performance, and handling business issues.
- **Project manager:** This position is responsible for creating project plans and managing IT projects.

Segregation of Duties

Information systems often process large volumes of information that is often highly valuable or sensitive. IT organizations should take measures to ensure that individuals do not possess sufficient privileges to carry out potentially harmful actions on their own. Checks and balances are needed so that high-value and high-sensitivity activities involve the coordination of two or more authorized individuals. The concept of segregation of duties (SOD), sometimes known as separation of duties, ensures that single individuals do not possess excess privileges that could result in unauthorized activities such as fraud or the manipulation, exposure, or compromise of sensitive data.

The concept of SOD has long been established in organization accounting departments, where, for instance, separate individuals or groups are responsible for the creation of vendors, the request for payments, and the remittance of payments. Since accounting personnel frequently handle checks, currency, and other payment instruments, the principles and practices of SOD controls in accounting departments are the norm.

IT departments are lagging behind somewhat, because the functions in IT are less often involved in direct monetary activities, except in some industries such as banking. But thanks to financial scandals in the 1980s and 1990s that involved the illicit manipulation of financial records and the emergence of new laws such as Sarbanes–Oxley, the need for full and formal IT-level SOD is now well recognized.

In its most basic form, the rule of segregation of duties specifies that no single individual should be permitted or be able to perform high-value, high-sensitivity, or high-risk actions. Instead, two or more parties must be required to perform these functions.

Segregation of Duties Controls

Preventive and detective controls should be implemented to manage SOD matters. In many organizations, both the preventive and detective controls will be manual, particularly when it comes to unwanted combinations of access between different applications. However, in some transaction-related situations, controls can be automated, although they may still require intervention by others.

Examples of SOD controls include the following:

- **Transaction authorization:** Information systems can be programmed or configured to require two (or more) persons to approve certain transactions. Many of us see this in retail establishments, where a manager is required to approve a large transaction or a refund. In IT applications, transactions meeting certain criteria (for example, exceeding normally accepted limits or conditions) may require a manager's approval to be able to proceed.

- **Split custody of high-value assets:** Assets of high importance or value can be protected using various means of split custody. For example, a password to an encryption key that protects a highly valued asset can be split in two halves—one half assigned to two persons, and the other half assigned to two persons—so that no single individual knows the entire password. Banks do this for central vaults, where a vault combination is split into two or more pieces so that two or more people are required to open it.
- **Workflow:** Applications that are workflow-enabled can use a second (or third) level of approval before certain high-value or high-sensitivity activities can take place. For example, a workflow application that is used to provision user accounts can include extra management approval steps in requests for administrative privileges.
- **Periodic reviews:** IT or internal audit personnel can periodically review user access rights to identify whether any SOD issues exist. The access privileges for each worker can be compared against an SOD control matrix. Table 1.2 shows an example matrix.

When SOD issues are encountered during a review, management will need to decide how to mitigate the matter. The choices for mitigating an SOD issue include:

- **Reduce access privileges:** Management can reduce individual user privileges so that the conflict no longer exists.
- **Introduce a new control:** If management has determined that a person needs to retain privileges that are viewed as a conflict, then new preventive or detective controls need to be introduced that will prevent or detect unwanted activities. Examples of mitigating controls include increased logging to record the actions of personnel, improved exception reporting to identify possible issues, reconciliations of datasets, and external reviews of high-risk controls.

In addition to mitigating the SOD issue on a go-forward basis, a review should be performed to ensure that the SOD issue was not maliciously or unintentionally exploited.

An organization should periodically review its SOD matrix, particularly if new roles or high-value applications are added or changed.

Maintaining an Existing Program

Once an organization has an existing information security program, information security managers must operate and maintain that program. This involves monitoring the program to ensure that it remains in alignment with business objectives and the information security strategy as well as providing regular reporting to stakeholders.

TABLE 1.2 Example segregation of duties matrix identifying forbidden combinations of privileges (designated by an X)

	Management	Systems Analyst	SW Developer	SW Test	DB Admin	Systems Admin	Network Admin	Security Admin	Systems Operator	Helpdesk
Management		OK	X	X	X	X	X	X	X	X
Systems Analyst	OK		OK	X	X	X	X	X	X	X
SW Developer	X	OK		X	X	X	X	X	X	X
SW Test	X	X	X		X	X	X	X	X	X
DB Admin	X	X	X	X		OK	X	X	X	X
Systems Admin	X	X	X	X	OK		OK	X	OK	OK
Network Admin	X	X	X	X	X	OK		X	X	X
Security Admin	X	X	X	X	X	X	X		X	X
Systems Operator	X	X	X	X	X	OK	X	X		OK
Helpdesk	X	X	X	X	X	OK	X	X	OK	

Metrics and Monitoring

Organizations evaluate their security programs through the use of metrics that assess the efficiency and effectiveness of critical security controls. Metrics are measurements that provide insight into the health of a security program both at a single point in time and on a long-term basis.

It's critical that organizations define the metrics and performance measurements they will use in advance of reporting the data. This ensures the integrity of the process and prevents cherry-picking of favorable results for reporting purposes.

Security programs use three primary types of metrics to demonstrate their effectiveness and the state of the organization's security controls. These key indicators offer program management and operational metrics that evaluate the effectiveness and efficiency of the information security program:

- Key performance indicators (KPIs) are metrics that demonstrate the success of the security program in achieving its objectives. KPIs are mutually agreed-upon measures that evaluate whether a security program is meeting its defined goals. Generally speaking, KPIs are a look back at historical performance, providing a measuring stick to evaluate the past success of the program.
- Key risk indicators (KRIs) are measures that seek to quantify the security risk facing an organization. KRIs, unlike KPIs and key goal indicators (KGIs), are a look forward instead of back. They attempt to show how much risk exists that may jeopardize the future security of the organization.

Key Performance Indicators (KPIs)

Every organization will have to define its own KPIs, but the Information Technology Infrastructure Library (ITIL) framework provides a good starting point. They offer nine KPIs that security programs may choose to leverage:

- Percentage of the decrease in security breaches reported to the service desk
- Percentage of the decrease in the impact of security breaches
- Percentage of the increase in SLAs with appropriate security clauses
- Number of preventive security measures the organization implemented in response to security threats
- Amount of elapsed time between the identification of a security threat and the implementation of an appropriate control
- Number of major security incidents
- Number of security incidents that created service outages or impairments
- Number of security test, training, and awareness events that took place
- Number of shortcomings identified during security tests

Key Risk Indicators (KRIs)

KRIs also must be customized to the needs of the organization. ISACA recommends selecting KRIs based on four criteria:

- The potential impact of the KRI, or the likelihood that the indicator will identify potential risks that are significant to the business
- The effort required to implement, measure, and support the indicator on an ongoing basis
- The reliability of the indicator as a good predictor of risk
- The sensitivity of the indicator, meaning that it is able to accurately capture variances in the risk

Selecting and monitoring a strong set of KPIs and KRIs provides business and technology leaders with a solid assessment of the state of their security programs.

Reporting

Information security managers are responsible not only for developing and monitoring the key metrics of their security programs, but also for ensuring that key stakeholders remain aware of the program's status.

One common mistake made by information security managers is to develop a dashboard or web page with updated metrics and then simply inform stakeholders that they may view those metrics whenever they like. This approach may seem open and transparent, but it suffers from two major drawbacks:

- Stakeholders who are not involved in security on a day-to-day basis are unlikely to revisit the site unless prompted to do so periodically.
- Providing metrics is only one piece of the picture. Security managers should also provide context around those metrics to explain changes and update stakeholders on the progress of the program.

Managers should compile and present reports to key stakeholders on the activities, trends, and overall effectiveness of the information security program and underlying business processes. They may do this using formal written reports, in-person or recorded briefings, and/or informal email updates. In most cases, managers will use a mixture of these methods in a manner that is appropriate for the needs and culture of their organization.

Auditing IT Governance

IT governance is more about business processes than it is about technology. This will make audits of IT governance rely more on interviews and documentation reviews than on inspections of information systems. Effective or ineffective IT governance is discernible in interviews of IT personnel as well as of business customers and end users.

Exam Tip

Governance questions on the exam will consider ISACA's COBIT strategies as the standard but will be generic enough in nature to ensure that an understanding of other common IT governance methods will remain applicable to the test-taker. Focus here on the measures and instruments used to validate the governance model.

Problems in IT governance will manifest themselves through a variety of symptoms:

- **Discontent among staff or end users:** Burned-out or overworked IT staff, low IT morale, high turnover, and malaise among end users about IT-supported systems can indicate an IT department that lacks maturity and is falling behind on its methodology or is applying Band-Aid fixes to systems.
- **Poor system performance:** Excessive incidents of unscheduled downtime, a large backlog of support tasks, and long wait times indicate a lack of attention to the quality of applications.
- **Nonstandard hardware or software:** A mix of hardware or software technologies among applications or end-user systems may indicate a lack of technology standards or the failure to enforce standards that are already in place.
- **Project dysfunction:** An IT department suffering from late projects, aborted projects, and budget-busting projects indicates a lack of program and project management discipline.
- **Highly critical personnel:** A disproportionate overreliance on a few IT personnel indicates that responsibilities are not fairly apportioned over the entire IT staff. This may be a result of a lack of training, unqualified personnel, or high turnover.

Auditing Documentation and Records

The heart of an IT audit is the examination of documentation and records. They tell the story of IT control, planning, and day-to-day operations. When auditing IT governance, the IS (information systems) auditor will need to review many documents:

- **IT charter, strategy, and planning:** These documents will indicate management's commitment to IT strategic planning as a formally required activity. Other documents that should be requested include IT steering committee meeting agendas, minutes, and decision logs.
- **IT organization chart and job descriptions:** These documents give an indication of the organization's level of maturity regarding the classification of employees and their specific responsibilities. An org chart also depicts the hierarchy of management and control. Job description documents describe detailed responsibilities for each position in the IT organization. An IS auditor's interviews should include some inquiry into the actual

skills and experience of IT personnel to determine whether they correspond to their respective job descriptions.

- **HR/IT employee performance review process:** The IS auditor should review the process and procedures used for employee performance reviews. In particular, the IS auditor should view actual performance goals and review documents to see how well individual employees' goals align with IT department objectives. Further, any performance problems identified in performance reviews can be compared with documents that describe the outcomes of key IT projects.
- **HR promotion policy:** It will be helpful for the IS auditor to determine whether the organization has a policy (written or not) of promoting from within. In other words, when positions become available, does the organization first look within its ranks for potential candidates, or are new hires typically outsiders? This will influence both employee morale and the overall effectiveness of the IT organization.
- **HR manuals:** Documents such as the employee handbook, corporate policies, and HR procedures related to hiring, performance evaluation, disciplinary action, and termination should exist; reflect regular management reviews; and reflect practices that meet the organization's business needs.
- **Life cycle processes and procedures:** Processes such as the software development life cycle and change management should reflect the needs of IT governance. The IS auditor should request records from the SDLC (specifically, documents that describe specific changes to IT systems and supporting infrastructure) and change management process to see how changes mandated at the steering group level are carried out.
- **IT operations procedures:** IT operations process documents for activities such as service desk, monitoring, and computer and network operations should exist. The IS auditor should request records for these activities to determine whether these processes are active.
- **IT procurement process:** An IT organization needs to take a consistent and effective approach to the procurement process. The process should reflect management's attention to requirements development, bidding, vendor selection, and due diligence so that any supplier risks are identified and mitigated in the procurement phase and reflected in the service agreement contract. The goods and services provided by suppliers should be required to adhere to the organization's IT policies, processes, and standards; exceptions should be handled in an exception process. Records should exist that reflect ongoing attention to this process.
- **Quality management documents:** An IT organization that is committed to quality and improvement will have documents and records to support this objective.
- **Business continuity and disaster recovery documents:** These include documents such as the business impact assessment, critical assessment, and statements of impact, as well as evidence of periodic updates to recovery documentation and regular testing. Audits of business continuity and disaster recovery planning are covered in Chapter 6.

Another indication of a healthy governance system is evidence of regular review and update of all of these documents. Best practice would be to perform an annual review. Often this is found in each document's modification history, but it may also be present in a separate document management system.

Like any other facets of an audit, the IS auditor needs to conduct several interviews and walkthroughs to gain a level of confidence that these documents reflect the actual management and operations of an IT organization. These interviews should include staff from all levels of management, as well as key end users who can also attest to IT's organization and commitment to its governance program and the maturity of its processes.

The IS auditor should also review the processes related to the regular review and update of IT governance documents. Regular reviews attest to active management involvement in IT governance. The lack of recent reviews might suggest that management began a governance program but subsequently lost interest in it.

Auditing Contracts

The IS auditor who is examining IT governance needs to examine the service agreements between the organization and its key IT-related suppliers. Contracts should contain several items:

- **Service levels:** Contracts should contain a section on acceptable service levels and the process followed when service interruptions occur. Service outages should include an escalation path so that management can obtain information from appropriate levels of the supplier's management team.
- **Quality levels:** Contracts should contain specifications on the quality of goods or services delivered, as well as remedies when quality standards are not met.
- **Right to audit:** Contracts should include a right-to-audit clause that permits the organization to examine the supplier's premises and records upon reasonable notice.
- **External audits:** Contracts should include provisions that require the supplier to undergo appropriate and regular external audits. Audit reports should be available upon request, including remediation plans for any significant findings found in audits.
- **Conformance to security policies:** Suppliers should be required to provide goods or services that can meet the organization's security policies. For instance, if the organization's security policy requires specific password-quality standards, then the goods or services from suppliers should be able to meet those standards.
- **Protection and use of sensitive information:** Contracts should include detailed statements that describe how the organization's sensitive information will be protected and used. This is primarily relevant in an online, SaaS, or application service provider (ASP) model, where some of the organization's data will reside on systems or networks that

are under the control of a supplier. The contract should include details that describe how the supplier tests its controls to ensure that they are still effective. Third-party audits of these controls may also be warranted, depending on the sensitivity of the information in question.

- **Compliance with laws and regulations:** Contracts should require that the supplier conform to all relevant laws and regulations, including those that the organization itself is required to comply with; in other words, compliance with laws and regulations should flow to and include suppliers. For example, if a health care organization is required to comply with HIPAA, any suppliers that store or manage the organization's health care–related information must also be required to be in compliance with HIPAA regulations.
- **Incident notification:** Contracts should contain specific language that describes how incidents are handled and how the organization is notified of incidents. This includes not only service changes and interruptions, but also security incidents. The supplier should be required to notify the organization within a specific period, and also required to provide periodic updates as needed.
- **Source code escrow:** If the supplier is a software organization that uses proprietary software as a means for providing services, the supplier should be required to deposit its software source code regularly into a software escrow. A software escrow firm is a third-party organization that will place software into a vault and release it to customer organizations in the event of the failure of the supplier's business.
- **Liabilities:** Contracts should clearly state which parties are liable for which actions and activities. They should further specify the remedies available should any party fail to perform adequately.
- **Termination terms:** Contracts should contain reasonable provisions that describe the actions to be taken if the business relationship is terminated.

Although the IS auditor may not be required to understand the nuances of legal contracts, the auditor should look for these sections in contracts with key suppliers. The IS auditor should also look for other contractual provisions in supplier contracts that are specific to any unique or highly critical needs that are provided by a supplier.

Auditing Outsourcing

When an auditor is auditing an organization's key processes and systems, those processes and systems that are outsourced require just as much (if not more) scrutiny than if they were performed by the organization's own staff using its own assets. However, it may be difficult to audit the services provided by a third-party supplier, for several reasons:

- **Distance:** The supplier may be located in a remote region, and travel to the supplier's location may be costly.

- **Lack of audit contract terms:** The organization may not have a clause in its contract with the supplier that requires cooperation with auditors. While it may be said that the organization should have negotiated a right-to-audit clause, this point may be moot at the time of the audit.
- **Lack of cooperation:** The supplier might not cooperate with the organization's auditors. Noncooperation takes many forms, including taking excessive time to return inquiries and providing incomplete or inadequate records. An audit report may include one or more findings (nonconformities) related to the lack of cooperation; this may provide sufficient leverage to force the supplier to improve its cooperation or for the organization to look for a new supplier.

In an ideal situation, a supplier undergoes regular third-party audits that are relevant to the services provided and the supplier makes those audit results available on request. It is also important for an organization to have controls and review procedures for any outsourced processes.

Summary

IT governance is the top-down management and control of an IT organization. Governance is usually undertaken through a steering committee that consists of executives from throughout the organization. The steering committee is responsible for setting overall strategic direction and policy, ensuring that IT strategy is in alignment with the organization's strategy and objectives. The wishes of the steering committee are carried out through projects and tasks that steer the IT organization toward strategic objectives. The steering committee can monitor IT progress through a balanced scorecard.

The IT steering committee is responsible for IT strategic planning. The IT steering committee will develop and approve IT policies and appoint managers to develop and maintain processes, procedures, and standards, all of which should align with one another and with the organization's overall strategy.

Security governance is accomplished using the same means as IT governance; it begins with board-level involvement that sets the tone for risk appetite and is carried out through the chief information security officer (CISO) or chief information risk officer (CIRO), who develops security and privacy policies as well as strategic security programs, including incident management, vulnerability management, and identity and access management.

Enterprise architecture provides a meaningful way to depict complex IT environments in functional terms. The Zachman Framework is most often used to represent IT architecture in various layers of detail. Similarly, data flow diagrams illustrate the relationship between IT applications.

Risk management is the practice of identifying key assets and the vulnerabilities they may possess and the threats that may harm them if permitted. This is accomplished through a risk assessment that identifies assets, threats, and vulnerabilities in detail, and is followed by specific risk treatment strategies used to mitigate, transfer, avoid, or accept risks.

A risk assessment may be qualitative, where threats and risks are labeled on scales such as "high," "medium," and "low"; or it may be quantitative, where risks are expressed in financial terms.

Key management practices will help ensure that the IT organization will operate effectively. These practices include personnel management, which encompasses the hiring, development, and evaluation of employees, as well as onboarding and offboarding processes, and development of the employee handbook and other policies. Another key practice area is sourcing, which is the management of determining where and by whom key business processes will be performed; the basic choices are insourced or outsourced and on-site or offsite. The third key practice area is change management, the formal process whereby changes are applied to IT environments in a way that reduces risk and ensures highest reliability. The next practice area is financial management, a key area, given that IT organizations are cost-intensive and require planning and analysis to guarantee the best use of financial resources. Another practice area is quality management, where processes are carefully measured and managed so that they may be continuously improved over time. Another practice is portfolio management, which is the systematic management of IT projects, investments, and activities. The next key practice is controls management, which is oversight of the life cycle of activities related to the creation, measurement, and improvement of controls. The next practice area is security management, which encompasses several activities, including risk assessments, incident management, vulnerability management, access and identity management, compliance management, business continuity planning, and performance and capacity management.

The IT organization should have a formal management and reporting structure, as well as established roles and responsibilities and written job descriptions. Roles and responsibilities should address the need for segregation of duties to ensure that high-value and high-risk tasks are carried out by two or more persons and recorded.

Exam Essentials

Know how metrics are used to assess the efficiency and effectiveness of the information security program. Key performance indicators (KPIs) are metrics that demonstrate the success of the security program in achieving its objectives. KPIs look at historical performance. Key goal indicators (KGIs) measure progress toward defined goals. Key risk indicators (KRIs) try to quantify the security risk facing an organization. KRIs look forward at future potential risks.

Understand the roles and responsibilities for IT governance. IT executives and the board of directors are responsible for imposing an IT governance model encompassing IT strategy, information security, and formal enterprise architectural mandates. Strategic planning is accomplished by a steering committee, addressing the near-term and long-term requirements aligning business objectives and technology strategies.

Know the role that governance documents play in an organization. Policies, procedures, and standards enable validation of business practices against acceptable measures of regulatory compliance, performance, and standard operational guidelines.

Describe the purpose of a risk management program. Risk management involves the identification of potential risks and the appropriate responses for each risk based on impact assessment using qualitative and/or quantitative measures for an enterprise-wide risk management strategy.

Know the responsibilities of IT managers. Assigned IT management roles ensure that resource allocation, enterprise performance, and operational capabilities coordinate with business requirements by validating alignment with standards and procedures for change management and compliance with sourcing, financial, quality, and security controls.

Describe the purpose of an organizational structure. Formal organizational structure ensures alignment between operational roles and responsibilities within the enterprise, where a separation of duties ensures individual accountability and validation of policy alignment between coordinated team members.

Understand the role of auditing in the IT governance process. Regular auditing of the IT governance process ensures alignment with regulatory and business mandates in the evolving enterprise by ensuring that all documentation, contracts, and sourcing policies are reviewed and updated to meet changes in the living enterprise.

Review Questions

1. IT governance is most concerned with:
   - **A.** Security policy
   - **B.** IT policy
   - **C.** IT strategy
   - **D.** IT executive compensation

2. What is one of the advantages of outsourcing?
   - **A.** It permits the organization to focus on core competencies.
   - **B.** It results in reduced costs.
   - **C.** It provides greater control over work performed by the outsourcing agency.
   - **D.** It eliminates segregation of duties issues.

3. An external IS auditor has discovered a segregation of duties issue in a high-value process. What is the best action for the auditor to take?
   - **A.** Implement a preventive control.
   - **B.** Implement a detective control.
   - **C.** Implement a compensating control.
   - **D.** Document the matter in the audit report.

4. An organization has chosen to open a business office in another country where labor costs are lower and has hired workers to perform business functions there. This organization has:
   - **A.** Outsourced the function
   - **B.** Outsourced the function offshore
   - **C.** Insourced the function on-site
   - **D.** Insourced the function at a remote location

5. A company has been experiencing high IT staff turnover, long wait times for support, and discontent among end users regarding IT-supported systems. For an IT auditor, which of the following would be the most appropriate initial action to investigate these issues?
   - **A.** Review the IT department's project management methodologies.
   - **B.** Conduct interviews with IT personnel and end users.
   - **C.** Analyze the organization's hardware and software standards.
   - **D.** Evaluate the company's business continuity and disaster recovery plans.

6. An organization needs to better understand whether one of its key business processes is effective. What action should the organization consider?
   - **A.** Audit the process.
   - **B.** Benchmark the process.
   - **C.** Outsource the process.
   - **D.** Offshore the process.

7. Annualized loss expectancy (ALE) is defined as:
   - **A.** Single loss expectancy (SLE) × annualized rate of occurrence (ARO)
   - **B.** Exposure factor (EF) × the annualized rate of occurrence (ARO)
   - **C.** Single loss expectancy (SLE) × the exposure factor (EF)
   - **D.** Asset value (AV) × the single loss expectancy (SLE)

8. A quantitative risk analysis is more difficult to perform because:
   - **A.** It is difficult to get accurate figures on the impact of a realized threat.
   - **B.** It is difficult to get accurate figures on the probability of specific threats.
   - **C.** It is difficult to get accurate figures on the value of assets.
   - **D.** It is difficult to calculate the annualized loss expectancy of a specific threat.

9. During an IT governance audit, you notice that several projects have been aborted and many others have exceeded their budgets. Which document would most likely provide insight into the underlying causes of these project dysfunctions?
   - **A.** IT procurement process records
   - **B.** IT organization chart and job descriptions
   - **C.** IT steering committee meeting agendas and minutes
   - **D.** HR promotion policy documents

10. What is the purpose of a balanced scorecard?
   - **A.** Measures the efficiency of an IT organization
   - **B.** Evaluates the performance of individual employees
   - **C.** Benchmarks a process in the organization against peer organizations
   - **D.** Measures organizational performance and effectiveness against strategic goals

11. An organization has discovered that some of its employees have criminal records. What is the best course of action for the organization to take?
   - **A.** Terminate the employees with criminal records.
   - **B.** Immediately perform background checks, including criminal history, on all existing employees.
   - **C.** Immediately perform background checks, including criminal history, on all new employees.
   - **D.** Immediately perform background checks on those employees with criminal records.

12. What are the options for risk treatment?
   - **A.** Risk mitigation, risk reduction, and risk acceptance
   - **B.** Risk mitigation, risk reduction, risk transfer, and risk acceptance
   - **C.** Risk mitigation, risk avoidance, risk transfer, and risk acceptance
   - **D.** Risk mitigation, risk avoidance, risk transfer, and risk conveyance

13. An IS auditor is examining the IT standards document for an organization that was last reviewed two years earlier. What is the best course of action for the IS auditor?

- **A.** Locate the IT policy document and see how frequently IT standards should be reviewed.
- **B.** Compare the standards with current practices and make a determination of adequacy.
- **C.** Report that IT standards are not being reviewed often enough.
- **D.** Report that IT standards are adequate.

14. What is the most important step in the process of outsourcing a business function?

- **A.** Developing a business case
- **B.** Measuring the cost savings
- **C.** Measuring the change in risk
- **D.** Performing due diligence on the external service provider

15. An organization has published a new security policy. What is the best course of action for the organization to undertake to ensure that all employees will support the policy?

- **A.** The company CEO should send an email to all employees, instructing them to support the policy.
- **B.** The company should provide training on the new security policy.
- **C.** The company should publish the policy on an internal website.
- **D.** The company should require all employees to sign a statement agreeing to support the policy.

16. After completing the first year of his security awareness program, Charles reviews the data about how many personnel completed training compared to how many were assigned the training to determine whether he hit the 95 percent completion rate he was aiming for. What is this type of measure called?

- **A.** A KPI
- **B.** A metric
- **C.** An awareness control
- **D.** A return on investment rate

17. An accounting employee at Doolittle Industries was recently arrested for participation in an embezzlement scheme. The employee transferred money to a personal account and then shifted funds around between other accounts every day to disguise the fraud for months. Which one of the following controls might have best allowed the earlier detection of this fraud?

- **A.** Separation of duties
- **B.** Least privilege
- **C.** Defense in depth
- **D.** Mandatory vacation

18. Sally is developing a set of metrics that will help her organization assess changes in the threat environment and adjust their security program accordingly. What type of metrics is she developing?

A. KMIs

B. KGIs

C. KRIs

D. KPIs

19. The Acme Widgets Company is putting new controls in place for its accounting department. Management is concerned that a rogue accountant may be able to create a new false vendor and then issue checks to that vendor as payment for services that were never rendered. What security control can best help prevent this situation?

A. Mandatory vacation

B. Separation of duties

C. Defense in depth

D. Job rotation

20. Bob is developing a set of measures designed to evaluate how well the information security program in his organization is functioning. He will provide monthly reporting on these metrics, looking back at the program's functioning over the past month. What term best describes these metrics?

A. KMIs

B. KGIs

C. KRIs

D. KPIs