Chapter 1

# Governance

This chapter covers CRISC Domain 1, "Governance," including the Organizational Governance and Risk Governance subdomains. The job practice for this domain is described by ISACA as follows:

*The governance domain interrogates your knowledge of information about an organization's business and IT environments, organizational strategy, goals and objectives, and examines potential or realized impacts of IT risk to the organization's business objectives and operations, including Enterprise Risk Management and Risk Management Framework.*

The job practice consists of these elements:

## ✔ A—ORGANIZATIONAL GOVERNANCE

1. *Organizational Strategy, Goals, and Objectives*
2. *Organizational Structure, Roles, and Responsibilities*
3. *Organizational Culture*
4. *Policies and Standards*
5. *Business Processes*
6. *Organizational Assets*

## ✔ B—RISK GOVERNANCE

1. *Enterprise Risk Management and Risk Management Framework*
2. *Three Lines of Defense*
3. *Risk Profile*
4. *Risk Appetite and Risk Tolerance*
5. *Legal, Regulatory, and Contractual Requirements*
6. *Professional Ethics of Risk Management*

The CRISC Task Statements relevant to this domain focus on governance and how it applies in this context to the organization, particularly executive management.

**The CRISC Task Statements covered in this chapter are:**

1. ***Collect and review existing information regarding the organization's business and IT environments.***
2. ***Identify potential or realized impacts of IT risk to the organization's business objectives and operations.***
7. ***Facilitate the identification of risk appetite and risk tolerance by key stakeholders.***
22. ***Evaluate alignment of business practices with risk management and information security frameworks and standards.***

The topics in this chapter represent 26% of the CRISC examination. This chapter explores the governance aspects of risk for an organization, as well as the relationships between enterprise risk and IT risk. The chapter also examines risk management governance and its implementation within the organizational structure and culture. Governance also encompasses overall laws, regulations, and risk frameworks, which are discussed in detail. During these governance discussions, both external governance and internal governance, including their policies and standards, will be explained.

Internal governance also encompasses management oversight, including business process reviews, risk appetite, and tolerance, as well as contractual obligations related to risk management. Other topics related to the Task Statements touched on here and examined in depth in other chapters include elements of risk, such as assets and their value, threats, vulnerabilities, likelihood, and impact.

Although many organizations will "do the right thing" in terms of due diligence and care, upholding their legal and ethical responsibilities, many other organizations don't do it to the same standards. This is why governance is crucial to an organization. Governance ties all these elements together. Governance sets standards—whether they are legal, ethical, or otherwise—and attempts to "standardize" what organizations do in terms of their obligations to stakeholders and society in general. As you'll see in this chapter, governance drivers originate from various sources, both within and outside the organization. It is a synthesis of enforced requirements and organizational leadership culture. Additionally, governance is essential to ensure that organizations handle systems and data with care and fulfill their due diligence and due care obligations when managing data protection and risk.

This chapter focuses on organizational governance and its application to all the various elements of an information security management system, including mission, strategy, goals and objectives, roles and responsibilities, culture, risk, and ethics.

# Organizational Governance

*Governance* is the glue that holds all the different elements of an organization together, including its mission, strategy, goals, objectives, and operations. Governance establishes the policies and requirements an organization must meet and consists of both internal and external governance. External inputs come in the form of laws, regulations, professional and

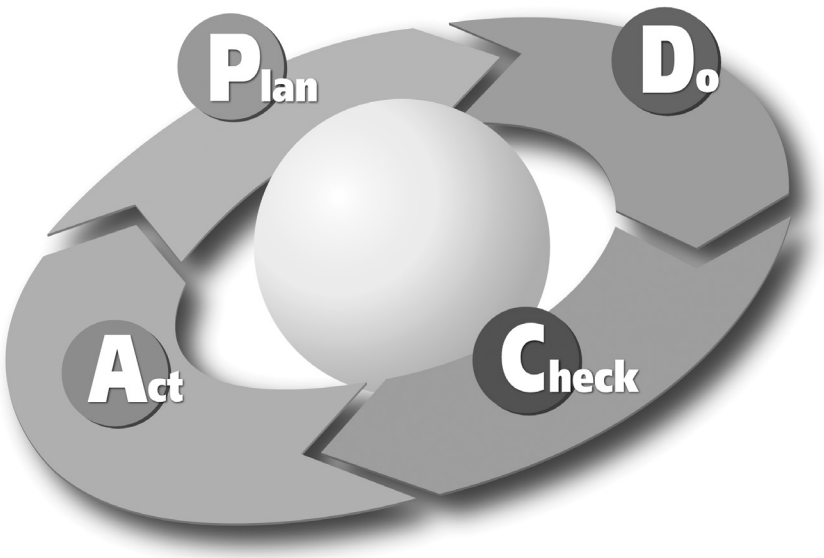
industry standards, and other sources of requirements imposed on the organization from the outside. Internal inputs typically support external inputs through policies, procedures, and processes. For example, if a law imposes requirements to protect certain sensitive data using specific controls or to a certain standard, then policies and procedures further support those requirements by formalizing and codifying them within the organization. Policies and procedures can also be independent of external governance and simply reflect the organization's culture, needs, and values, usually established by its executive management. In any event, governance is the controlling factor for the organization; it keeps the organization on the right track and ensures that it meets its compulsory requirements, such as adherence to laws, as well as fulfilling its due diligence and due care responsibilities.

In addition to imposing requirements on the organization, governance also refers to the structure by which the organization is led and regulated. Again, this can come from external or internal sources. External drivers for governance may include an external board of directors or regulatory agencies, which ensure that the organization is led with a focus on responsibility and accountability. Internal governance drivers originate from internal business leaders and reflect business drivers unrelated to externalities. In reality, good governance typically demonstrates a balance between internal and external business drivers.

Industry IT governance frameworks serve as models for organizations building or improving their governance structures. COSO ERM 2017, NIST RMF, ISO 31000, and COBIT 2019 are governance framework models that outline standard approaches for aligning IT strategies with business strategies to maintain shareholder value. Governance is a *lifecycle* process, modeled after the *Deming Cycle*, which is depicted in Figure 1.1.

The organizational infrastructure framework, encompassing strategy, goals, objectives, mission statements, and other elements, supports governance, as discussed further in this chapter.

**FIGURE 1.1** The Deming Cycle depicts a typical lifecycle process.




*Source:* Image from Karn Bulsuk (`www.bulsuk.com`).

## Organizational Strategy, Goals, and Objectives

Every organization operates with a *mission* that defines its purpose and long-term direction. The organization is in business for a particular purpose, not merely because people want to come to work every day to perform tasks and socialize. Missions, goals, and objectives directly relate to why the organization is in business in the first place, whether that is to develop and market a product or provide a service. Organizational senior management defines the business's mission, goals, and objectives, typically on a strategic or long-term level. Senior management also determines the levels of risk tolerance, appetite, and capacity (discussed later in this chapter), based on factors such as the market space, operational environment, economy, and governmental regulations. These risk levels directly align with and support the business mission, balancing business opportunities that can generate revenue and move the business forward with potential adverse events that may cause the business to fail or at least have a detrimental impact on the organization.

One of the critical characteristics of governance structures is their *business alignment*, which refers to the degree to which those structures support the organization's mission, goals, policies, and culture. Processes and policies that are business-aligned will work with better harmony in the organization than those that are not.

Risk appetite and tolerance are directly related to the business mission, although different business pursuits may have varying levels of each. Senior management sets those levels based on the potential rewards from risky opportunities and the amount of loss the organization could endure if those rewards don't materialize.

## Organizational Structure, Roles, and Responsibilities

How the business is organized can help drive how it deals with risk in several ways. Most businesses are organized from a functional perspective; in other words, departments and other hierarchical structures are established to handle specific functions that contribute to the business's goals and objectives. Also, organizational structure determines how authority and responsibility are distributed.

An organization's board of directors provides ultimate oversight and often establishes specialized committees such as audit, risk, technology, or ESG (environmental, social, and governance). Executive management implements governance through an enterprise risk and control structure. The Chief Executive Officer (CEO) aligns strategy with risk appetite, the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) manage technology and security risk, the Chief Risk Officer (CRO) oversees the enterprise risk framework, and the Data Protection Officer (DPO) manages data and privacy compliance. In technology-driven organizations, a Chief AI Officer (CAIO) may oversee responsible artificial intelligence (AI) practices.

For example, in a production-driven business, there may be a manufacturing or production department, an engineering department, a research and development department,

and an assembly line. There will likely be additional departments that cover support functions, such as marketing, accounting and finance, public relations, and so on. A hospital, on the other hand, will be organized according to its specific functions, such as the emergency department, surgery, neurology, radiology, and so on. Businesses in other markets or areas will be organized differently as well. In any case, the organization of the business is structured as its mission and business purposes dictate. Certain functions can be found in any business, such as information technology, information security, and even legal compliance. These functional areas may have the primary function of dealing with risk. Still, it is also essential to consider that all organizational structures, from lower-level work sections to higher-level departments and divisions, have responsibilities regarding risk management.

The organization must examine its structure and determine how each unit will manage risk at its own level, recognizing that risk management should be uniform throughout the entire organization and explicit at all levels. Business unit leaders identify and manage risks within their domains, while risk and compliance professionals provide guidance and oversight. For example, risks that the accounting department incurs are only a subset of the risks at higher organizational levels and are incorporated into their risk management processes. Each lower-level unit in an organizational hierarchy has risks that are part of the next higher level's risk considerations. While individual units may be responsible for only a small piece of the overall organizational risk, their parent units also bear responsibility for managing that risk, as well as the risk of other subordinate units. Another concept related to organizational structures is that all parts of the organization bear the risk incurred by any part of the organization; there is almost no risk that only affects a small part of the business. Risk ripples across the entire organization in some way.

Each unit, whether it is located in the lower levels of the business hierarchy or at the highest levels, should take steps to identify, evaluate, and assess risks at its respective level. Risks can be categorized into tactical, operational, and strategic levels. *Tactical risks* are those short-term risks that are encountered by smaller-level production sections—those that carry out the day-to-day work of the organization. *Operational risks* are medium-term risks that can span multiple work units and relate to how the business conducts its functions, as well as how the various work units interact. *Strategic risk* is long-term risk borne at the higher levels of the organization, including senior management. It involves risks incurred by leading the business toward opportunities and away from decisions that exceed the organization's risk appetite and tolerance. Respectively, these three types of risks also correspond to short-term, medium-term, and long-term risks.

Regardless of the level of risk incurred within the organization, there should be an enterprise risk management strategy and program in place to deal with the lower-tier, middle-tier, and higher-tier risks as well as ensure that the risk management strategy handles risks consistently and uniformly in alignment with the organization's risk tolerance and appetite. Governance at higher levels of the organization influences risk appetite and tolerance, shaping the organization's risk management strategy throughout the organization. The organizational structure must support that governance, as well as clearly define lines of authority and responsibility in terms of risk leadership and management.

**Selecting Stakeholders for the Cyber Risk Governance Committee**

A software-as-a-service (SaaS) organization recently hired a new CISO to make strategic improvements to cybersecurity risk management. Experienced in risk management and risk governance, the CISO assessed the current state of cybersecurity and risk management.

The CISO interviewed senior executives and department heads to understand their opinions and concerns about cyber risk management in the organization. The CISO needed to know how the organization works, as well as the attitudes of those interviewed.

The CISO identified key *stakeholders*, including the CIO, heads of HR, legal, product development, customer support, and finance, and explained to each of them how cyber risk management could be implemented within the organization without disrupting critical business processes.

Part of the CISO's objective in these meetings was to learn from these leaders, and to build trust with them. Without trust, new processes like cyber risk management are unlikely to succeed.

## Organizational Culture

Organizational *culture* is the term that describes how people treat each other, how they make decisions, and how they respond to risk. Many organizations establish a set of values that define the norms of behavior. Terms such as *respect*, *collaboration*, and *teamwork* are often reflected in these values. Some organizations publish formal *value statements* and display them in lobbies, offices, and conference rooms. Many also publish a code of conduct that defines the boundaries of ethical behavior.

The way that an organization's leaders treat each other and the rest of the organization sets an example for behavioral norms. Often, these norms reflect those formal values, but sometimes they may differ. One could say that an organization's stated culture and its actual culture may vary a little, or a lot. The degree of alignment itself reflects an organization's culture.

An organization also has a *risk culture*, which is essentially how the organization as an entity feels about and deals with risk. This culture is developed from several sources. First, it can come from the organization's leadership, based on their business and management philosophies, attitudes, education, and experience. It can also come from the organization's governance. Remember that governance is essentially the rules and regulations imposed on the organization by either external entities (in the form of laws, for example) or internally by the organization itself. In any case, the culture of the organization really defines how the organization feels about risk and how it treats risk over time. You will read later about how these two concepts—risk tolerance and risk appetite—support the organizational risk culture.

## Policies and Standards

Policies are the instruments through which governance intent becomes operational reality. They formalize management's directives regarding acceptable behavior, security requirements, and control expectations.

The most common policy hierarchy typically includes:

- ***Policy*:** Broad management statements of intent
- ***Standard*:** Mandatory requirements or specifications that support policy
- ***Process*:** A grouping of procedures that support a business function
- ***Procedure*:** Step-by-step instructions for performing tasks
- ***Guideline*:** Recommended practice for implementing a policy

Controls exist outside the policy hierarchy but are mapped to policies or derived from them. Different types of controls work together to protect an organization, many of which have a technical focus. However, while the more technical approaches are often the stars of the cybersecurity show, the importance of good old-fashioned policy cannot be overstated. Controls are discussed in detail in Chapter 3, "Risk Response and Reporting."

Without a policy, a security program often falls short due to a lack of governance, management involvement, and accountability. This objective covers different types of policies and how they work together to form the underlying foundation of human and process control, ensuring a balanced and effective security program.

To provide effective security, security policy and procedure creation must begin at the top of an organization, with senior management that understands, supports, and holds personnel accountable for adhering to the written policies. Remember that organizational policies must articulate governance, reflecting the requirements found in laws and regulations, as well as the management philosophies and tolerances of the organization's leadership. These policies and procedures must then flow throughout the organization to ensure that security is valued and functional at every level. Understanding organizational security must begin with an understanding of the fundamental laws, regulations, and legal jurisdiction that policies must be informed by to protect not only the organization and its assets but also its employees and customers.

Management creates policies based on its leadership philosophies, culture, industry standards and requirements, and, most importantly, external governance inputs. Policies articulate with all these items and represent management's directives in upholding these requirements. Policies specific to risk governance include a body of documents that may begin with the risk management strategy, which outlines the organization's overall strategy, methodology, and long-term objectives for managing risk. Policies support the strategy, as well as governance requirements, such as those that may be found in laws or regulations that dictate that certain risk management activities must take place within the organization. An example of a risk-related policy is a risk management or risk assessment policy, which outlines the organization's requirements for risk management, assessment, analysis, treatment, and monitoring. This policy may be brief or detailed, but will usually state roles and responsibilities, the risk management methodology adopted by the organization, and the requirement to implement detailed risk management procedures.

Policy governance follows a defined lifecycle: creation, approval, publication, review, and retirement. Policies must be endorsed by senior management and communicated across all levels. They should be reviewed periodically (annually is a good start), particularly when regulations, technologies, or business conditions change.

Modern organizations use automated policy management tools that track control status, regulatory mapping, and version history. Continuous compliance programs integrate policy enforcement with enterprise *integrated risk management (IRM)* (formerly known as governance, risk, and compliance [GRC]) systems.

Policies should align with external frameworks such as ISO/IEC (International Organization for Standardization and the International Electrotechnical Commission) 27001:2022, ISO/IEC 42001 (Artificial Intelligence Management System), National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, and/or other relevant frameworks. Mapping internal policies to these standards improves consistency and audit readiness.

## Business Processes

*Business processes* are structured activities that fulfill the organization's mission. Governance ensures that these processes operate efficiently, meet objectives, and remain within established risk boundaries.

Each process has an identified owner responsible for outcomes and associated risks. Process governance requires documentation of roles, dependencies, and control activities.

For example, a shoe manufacturer is in the business of making shoes; therefore, its mission is to make good-quality shoes. Most businesses have a mission statement that describes their mission. While the mission is the overall reason for existence, business processes are the activities that carry out that mission. A shoe manufacturer's business processes could be as high-level as manufacturing, sales, and marketing, but even those higher-level processes are broken down into smaller activities, such as sewing cloth and leather, developing types and styles of shoes, and selling them to retailers. These are all processes that support the business.

Each of these business processes also incurs some level of business risk. There could be risks in the manufacturing process due to the types of materials or a specific manner of attaching the shoe soles to the rest of the shoe. A faulty process could mean that the shoes are of lesser quality than other competitors or that the styles don't meet the demands of consumers, leading to fewer sales or more consumer returns. Regardless of whether they are higher-level processes or more detailed activities and tasks, each is supported by one or more systems or sets of data. These systems also incur risk, but of a different nature. The risk incurred by the systems includes the ability to effectively use those systems and data to support various business processes. Therefore, IT (or even cybersecurity) risk directly informs business process risk, as it can affect the organization's ability to carry out its business processes and, in turn, its overall mission.

Business processes should be "owned" by different managers within the organization, which means that business process owners are responsible for both the day-to-day and the long-term operations and success of the process. This also means that they are ordinarily

the primary owners of the business risk associated with the process. Of course, higher-level management also bears ownership and responsibility for both the process and risk; however, these are typically the people in charge of the business process.

Automation technologies, including robotic process automation and AI-assisted decision systems, can increase efficiency but introduce governance challenges related to control validation and transparency. Governance frameworks ensure that automation remains aligned with policy, ethics, and compliance expectations.

Better organizations will take a formal approach regarding the development and management of business processes. Documents that describe processes, roles and responsibilities, and key assets may be formally managed through business process change management and periodic review, and kept in official repositories to ensure that no unauthorized changes occur. Process *maturity* and capability can be evaluated using models such as the COBIT Process Assessment Model. Process maturity is the degree of formality and optimization in place for a business process. Continuous improvement involves periodic review, automation, and optimization. COBIT is discussed in detail in Chapter 4.

Measuring business processes in various ways supports governance effectiveness:

- Key Performance Indicators (KPIs) track output and efficiency.
- Key Risk Indicators (KRIs) measure exposure levels.
- Key Control Indicators (KCIs) assess whether controls perform as intended.

Organizations with higher maturity will develop metrics and KPIs associated with each business process, allowing management to understand the quantity and quality of business process output. This understanding can be used to identify tactical and strategic improvements that enhance the effectiveness and efficiency of processes. Risk practitioners must work together with business process owners to develop these KPIs, as well as KRIs and KCIs.


KPIs, as well as KRIs and KCIs, are covered in more detail in Chapter 3, which discusses risk response and reporting as part of CRISC Domain 3.

## Organizational Assets

Company *assets* can include physical items, such as computer and networking equipment, office machines (for example, scanners and copiers), work facilities, and information processing centers, as well as less tangible assets, such as software, business records, configuration data, license and activation keys, login credentials, and data. Asset governance provides the foundation for effective risk management and control of information systems. Asset identification involves identifying both types of assets and determining their value. Asset values must be established beyond the mere capital costs; an accurate asset valuation should consider several factors. For example, a consideration should be the cost of repairing or recovering the asset versus simply replacing it outright. Often, repairing the asset may be less expensive in the short run, but the cost of the different components required to conduct a repair should be

considered. Also, it's important to remember that this might only be a temporary solution—one that could come back to haunt you (and your budget) in the long run.

*Asset management* encompasses a range of activities designed to oversee the inventory, classification, utilization, and disposition of assets. Asset management is a foundational activity, without which several other activities could not be effectively done, including vulnerability management, device hardening, incident management, data security (these terms are discussed in Chapter 4), and some aspects of financial management.

In information security, asset management is critical to the success of vulnerability and attack surface management, which is discussed in Chapter 4. If assets are not known to exist, they may be excluded from processes used to identify and remediate vulnerabilities. Similarly, it will be difficult to harden assets if their existence is not known. Furthermore, if an unknown asset is attacked, the organization may have no way of directly realizing this in a timely manner. If an attacker compromises an unknown device, the attack may not be known until the attacker pivots and selects additional assets to compromise. This time lag could prove crucial to the impact of the incident.

The criticality of asset management warrants governance emphasis on these activities.


Senior executives in many organizations still do not fully understand the importance of maintaining a complete and accurate inventory of assets in the context of cybersecurity. In other contexts, incomplete asset inventories pose quality and financial efficiency issues. However, in the context of cybersecurity, failing to maintain an accurate inventory can permit existential threats to manifest and potentially destroy the business.

## Asset Identification

A security management program's primary objective (whether formally stated or not) is the protection of the organization's assets. These assets may be tangible or intangible, physical, logical, or virtual. Here are some examples of assets:

- **Buildings and property:** These assets include real estate, structures, and other improvements.
- **Equipment:** This can include machinery, vehicles, and office equipment such as copiers, printers, and scanners.
- **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.
- **Virtual assets:** In addition to the tangible IT equipment cited, virtual assets include virtual machines and the software running on them.
- **SaaS applications:** While owned and operated by external vendors, they perform functions critical to the organization. *Shared responsibility models* and contractual terms define vendor and customer roles and vary by service provider.

- **Supplies and materials:** These can include office supplies as well as materials used in manufacturing.
- **Records:** These include business records, such as contracts, video surveillance tapes, visitor logs, and more.
- **Information:** This includes data in software applications, documents, email messages, and files of all kinds on workstations and servers.
- **Intellectual property:** This includes an organization's designs, architectures, patents, software source code, processes, and procedures.
- **Personnel:** In a real sense, 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 refers to the individual and collective opinion about an organization held by its customers, competitors, shareholders, and the broader community.
- **Brand equity:** Similar to reputation, this refers to the perceived or actual market value of a brand, product, or service produced by the organization.

## Sources of Asset Data

An organization that is building or improving its security management program may need to build its asset inventory from scratch. Management will need to determine where this initial asset data will come from. Some sources include 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. However, it may not be entirely useful: 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 with assets in actual use may require more effort than other methods for creating the initial asset list. However, for organizations that have a relatively small number of highly valued assets (for instance, an ore 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 may not include the value of information stored on (or processed by) the asset.

- **Interviews:** Discussions with key personnel for the purpose 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. While this information may not encompass every IT

asset in the organization, it can provide information on the assets supporting individual applications or geographic locations.

- **Online data:** An organization with a large number of IT assets (systems, network devices, and so on) can sometimes utilize the capability of online data to identify those assets. An organization with cloud-based assets can utilize the asset management portion of the cloud services dashboard to determine the number and type of assets in use. Additionally, a systems or network management system often includes a list of managed assets, which can serve as a good starting point when creating the initial asset list.
- **Security scans:** An organization that has security scanning tools can use them to identify network assets. This technique will identify both authorized and unauthorized assets.
- **Asset management system:** Larger organizations may find it more cost-effective to use an asset management application dedicated to this purpose, rather than relying on lists of assets from other sources.

None of these sources should be considered accurate or complete. Instead, as a formal asset inventory is being assembled, the security manager should continue to explore other sources of assets.

## Collecting and Organizing Asset Data

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

When asset inventory is not prioritized, other risks emerge. From a consequence-based perspective, unidentified or unmanaged assets represent the highest level of criticality, since their existence outside of formal control boundaries, business processes, and tooling creates unknown exposure and unmitigated risk. While an unidentified asset may not play a critical role in business process support, its neglect may substantially increase risk—risk that may not be specifically identified, and yet it exists. In cybersecurity, this is informally known as *dark risk* or shadow risk.


As part of IT governance, management needs to determine who is responsible for maintaining asset inventories.

It is usually helpful to organize or classify assets, which helps identify assets 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 want to classify its assets according to their location, aiding risk managers during the risk analysis phase, since many risks are geographic-centric, particularly natural hazards.
- **Service provider:** An organization utilizing one or more infrastructure-as-a-service (IaaS) providers can group its assets by service provider.

- **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 they support. This classification helps 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 unit they support.
- **Sensitivity:** Usually ascribed to information, sensitivity relates to the nature and content of that information and its relative confidentiality. 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.
- **Criticality:** Whereas some assets may be classified according to their sensitivity, others may also be classified by their criticality (or both), which is their importance to the organization in terms of performing its mission. Not all assets are sensitive, but they may still be highly necessary for the organization to function. Conversely, not all assets are considered critical, but still could be classified as sensitive in terms of confidentiality. Note that assets could be considered either sensitive or critical, or both.
- **Regulation:** For organizations required to follow government and other legal obligations regarding the processing and protection of information, it will be helpful 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 helpful 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 analyst should collect several points of metadata about each asset (including location, process supported, and organizational unit supported). This will enable the security 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 use configuration management databases (CMDBs), discovery tools, and GRC-integrated asset registers to maintain visibility and accountability. Automated synchronization among asset, vulnerability, and compliance systems strengthens overall governance.

# Risk Governance

*Risk governance* has several different aspects. As mentioned earlier, governance outlines the overall requirements that the organization must adhere to, which may include legal, regulatory, ethical, safety, and professional standards. Risk governance, then, describes the requirements that an organization must adhere to in managing both business and IT risk. Laws, regulations, and other external inputs can dictate portions of risk governance, as can internal governance, which comes in the form of policy. Risk governance is also established

by executive management through the formation of risk appetite and tolerance, risk strategy, and through various policies that support risk management. Risk governance encompasses adopting a risk assessment and analysis methodology, risk treatment and response options, risk monitoring processes, and so on. Table 1.1 lists the various facets of risk governance and their coverage in this book.

**TABLE 1.1** The principal components of risk governance.

| Topic | Description | Coverage |
|---|---|---|
| Risk culture and leadership | Norms and behaviors | Chapter 1 |
| Enterprise risk management | Comprehensive risk on all topics, including cybersecurity | Chapter 1 |
| Risk management frameworks | Industry standard risk management methodologies | Chapter 1 |
| Three lines of defense | An industry standard assurance and accountability model | Chapter 1 |
| Risk appetite and risk tolerance | Thresholds that guide risk treatment decisions | Chapter 1 |
| Risk assessment and risk analysis | Industry standard risk assessment and risk analysis methodologies | Chapter 2 |
| Risk response and risk treatment | Decisions and follow-up on the disposition of identified risks | Chapter 3 |
| Control design and selection | The design, selection, and implementation of controls to reduce identified risks | Chapter 3 |
| Risk monitoring | Continuous and periodic risk assessments | Chapter 3 |
| Risk metrics and reporting | The development of metrics and reporting for senior management | Chapter 3 |
| Continuous improvement | Periodic updates to risk governance processes | Chapter 3 |
| Security policies, standards, and guidelines | Cybersecurity-related corporate policy defining expected behavior and characteristics | Chapter 5 |

## ERM and Risk Management Frameworks

*Enterprise risk management (ERM)* is the practice of identifying and managing strategic risk in an organization. Topics of ERM include macroeconomics, market risk, regulations, workforce, information technology, and cybersecurity. Individual risks in ERM will cite various uncertainties and scenarios that, if realized, may impede the organization's long-term viability.

Standards and frameworks help provide a standardized, industry-accepted approach toward managing risk. While they're certainly not perfect, they provide a baseline for an organization to recognize the key steps toward understanding and categorizing the risks to its business, implementing the appropriate security controls to lower risk to an acceptable level, and continually monitoring the residual risk and reporting the status to management. Each standard and framework has its own pluses and minuses, and this section discusses two of the more commonly used: the ISACA Risk IT Framework and the National Institute of Standards and Technology (NIST) Risk Management Framework. Keep in mind that this discussion is intended to introduce you to the frameworks.

### ISACA Risk IT Framework

Initially published in 2009, the ISACA *Risk IT Framework* is a widely recognized risk management framework you should be aware of. ISACA created a framework that merges the traditional IT models with a more risk-focused mindset. Within the ISACA model, the activities considered key are grouped into processes, which in turn are grouped into three domains. You will see many of the same concepts that you'll find within this book (and even this chapter), so it's definitely a worthwhile model to review. The domains are as follows:

- **Risk Governance:** Discusses risk appetite, risk tolerance, and communicating risk to leadership.
- **Risk Evaluation:** Includes an understanding of the impacts to the business and the risk scenarios, developed through the inclusion of internal and external environmental factors, risk management capability, IT capability, and IT-related business capability.
- **Risk Response:** Covers the risk response definition, risk response prioritization, and key risk indicators (KRIs).

The framework outlines risk response options, including risk avoidance, risk mitigation, risk sharing and transfer, and risk acceptance.

### NIST Risk Management Framework

*NIST* Special Publication 800-37, Revision 2, "Guide for Applying the Risk Management Framework to Federal Information Systems," along with other supporting publications from NIST (part of the U.S. Department of Commerce), make up the defining volumes of the *NIST Risk Management Framework (RMF)*. The RMF is composed of seven steps:

1. Prepare.
2. Categorize information systems.
3. Select security controls.

4. Implement security controls.
5. Assess security controls.
6. Authorize information systems.
7. Monitor security controls.

Security categorization requires the information systems and associated information to be categorized based on an analysis of the impact to the organization of a loss of confidentiality, integrity, and availability for the system. When selecting a set of security controls, you must consider both the security categorization and any previous risk assessments. Following this step, you implement the previously selected security controls and then assess their effectiveness and the overall success of the controls in reducing the risk to the accepted level. Finally, security controls must be continually monitored to ensure they continue to operate as intended. You also need to consider any changes that come into effect across the organization (think location, mission, security classification, or other underlying factors).

You will notice many additional concepts within NIST Special Publication 800-37 that are germane to the CRISC exam; for example, the early steps of the RMF discuss categorizing and selecting appropriate security controls (discussed later in the book), while other steps correspond to the implementation, assessment, and continuous monitoring of controls (covered throughout this book). For these reasons alone, it's a great idea to read this document to understand how the steps work together and how they are similar to (and sometimes different than) other frameworks.

## COSO Enterprise Risk Management

The *COSO Enterprise Risk Management (ERM) Framework* provides a structured approach for identifying, assessing, and managing risks in alignment with organizational strategy. It expands on COSO's internal control model to emphasize governance, culture, risk appetite, and performance integration. The framework consists of five interrelated components—governance and culture, strategy and objective-setting, performance, review and revision, and information, communication, and reporting—supported by 20 principles. COSO ERM promotes proactive risk management, enhancing decision-making and organizational value. The full framework and executive summary are available for purchase and download at `www.coso.org`.

## ISO 31000

ISO 31000 ("Risk Management—Guidelines") is an international risk management framework that provides a common approach for managing any type of risk in any-sized organization and in any industry sector. The standard outlines fundamental principles and processes for contextualizing and managing risk, as well as monitoring, reviewing, and continually improving risk management procedures. The standard is available for purchase at `www.iso.org`.

## Three Lines of Defense

The *three lines of defense* model is an industry practice for managing and operationalizing enterprise risk. The model defines three distinct, independent roles to ensure business operations are managed properly. The three roles are operational management, risk management and compliance, and internal audit. These roles are implemented at different levels of the organization, across business processes, as part of the wider enterprise risk management program. The personnel responsible for these three lines of defense roles are the risk owner, who is ultimately accountable and responsible for how risk is treated, and the risk practitioner, who is responsible for the day-to-day risk management functions.

The roles in the three lines of defense must be independent of one another, so that none of the roles can organizationally influence any other. Often, internal audit reports directly to the board of directors, while operations and risk are likewise separate from each other.

### Operational Management

Operational management refers to the tactical management activities that take place at the business unit or business process level. At this level, risk and controls are managed on a day-to-day basis by monitoring control effectiveness, as well as any risk associated with the business process itself or its supporting systems. This line of defense can be implemented by the risk practitioner, IT, or cybersecurity teams. Operations is the layer in which controls are operated as a part of business processes and often implemented as a part of information systems.

### Risk and Compliance

Risk and compliance management is a line of defense that involves proactively monitoring and managing risks associated with IT support systems, security policies that define expected behavior, security controls implemented to protect systems, and risks associated with overall business processes. This is where the organization's risk management program excels; implementing the activities associated with the risk governance framework is part of this critical line of defense. This includes overall risk assessment and analysis, risk response, and continuous risk monitoring.

Compliance management involves ensuring that the organization, its business processes, and the supporting IT systems comply with any governance requirements, whether they come from inside the organization or from external entities. Compliance directly leads to auditing processes and systems, discussed next.

While risk and compliance management are connected, they are separate and distinct entities. Risk can be variable in nature and changes over time, whereas compliance is typically a binary (yes/no, compliant/noncompliant) mentality. However, there is usually some overlap between these two areas, particularly in control assessments and risk analysis, as both risk management and compliance management often require control and risk assessments. Business process owners, senior managers, and senior risk practitioners are typically involved in this line of defense.

### Internal Audit and Accountability

In the world of risk management, auditing involves continuously monitoring risk levels to ensure they remain within acceptable levels of risk appetite and tolerance, as well as monitoring the controls, management processes, and responses that maintain acceptable risk levels. This could mean auditing at the process level (user account management, for instance) or even at the overall organizational risk level, and every area of interest in between. Auditing ensures that processes and activities are being conducted in accordance with governance and serves to further ensure accountability.

While auditing and accountability are not the same thing, they are related. Accountability, in the context of risk management, ensures that risk owners are both responsible and accountable for managing risk at an acceptable level within their designated area of responsibility. In short, accountability ensures they are doing their job. Accountability is connected to auditing in the respect that only through auditing processes and activities can you determine if those processes and activities are fulfilling the governance and risk management requirements that risk owners are responsible for meeting.

## Risk Profile

A *risk profile* encompasses an overall asset, organization, or business process under review. It includes detailed information on all aspects of those items and how they contribute to, mitigate, or influence risk. The risk profile for a system, for instance, would present detailed information on all the different characteristics of the system, its security controls, the risk assessment and analysis for the system, the risk responses for the system, and ongoing management for that risk. A risk profile typically consists of the following:

- Description of the asset, system, or process.
- Identified threats and vulnerabilities.
- Control inventory and effectiveness ratings.
- Likelihood and impact assessments.
- Residual risk and ownership assignment.
- Relevant regulatory or contractual obligations.

Risk profiles are dynamic: they change based on a variety of factors, including the criticality or sensitivity of the system, changes to business processes, the vulnerabilities inherent to the system, the threats that may exploit those vulnerabilities, the mitigating security controls that protect the system, and significant incidents. Regulations and societal norms also influence risk profile, particularly in areas such as data privacy. The risk profile is used to actively manage ongoing risk and ensure that it remains within acceptable levels.

## Risk Appetite and Risk Tolerance

As discussed previously, the culture of the organization really defines how the organization feels about risk and how it treats risk over time. *Risk capacity* refers to the amount of loss an organization can incur without significantly affecting its ability to continue. More resilient

organizations can endure greater loss than those that are less resilient. An organization's resilience can sometimes be informed by its *risk culture*, which is senior management's attitude about risk. As part of the organization's risk culture, there are its risk appetite and risk tolerance. These are different terms you also need to know to understand risk.

*Risk appetite* is, in effect, how much risk an organization is willing to deal with in any given endeavor. Risk appetite is the general level of risk that an organization is willing to accept in the course of its operations. An organization's risk appetite is driven by the corporate risk culture and by the environment in which the organization exists (market, regulation, and other external factors).

*Risk tolerance*, on the other hand, is the acceptable level of deviation in risk for a particular endeavor or business pursuit. Risk tolerance refers to the degree of variation from the expected level of risk that an organization is willing to accept. There's a certain amount of risk in every business enterprise or pursuit; however, the organization may not be able or willing to tolerate large deviations from what it considers its acceptable level of risk on an endeavor. Note that risk appetite is often determined for the entire organization as a whole, whereas risk tolerance typically applies to a specific business venture, such as bringing a new product to market, for instance.

The board and senior management jointly define risk appetite through facilitated workshops and quantitative assessments. Stakeholder engagement ensures that appetite and tolerance reflect the organization's mission, resources, and environment. Risk appetite and tolerance must evolve in response to changes in business strategy, market conditions, or regulatory expectations. Regular reassessment ensures alignment between governance intent and operational practice.


Understand the differences between risk appetite and risk tolerance; *risk appetite* involves how much risk the organization is willing to endure, whereas *risk tolerance* is how much variation from that amount is acceptable to the business for a particular venture. Risk culture drives both of these factors.

A healthcare provider declares that it has very little appetite for risks that could expose patient health information. This strategic position reflects regulatory obligations, reputational concerns, and the high number of attacks on healthcare organizations. To ensure that operations stay within this boundary, the security team sets specific tolerance levels for system vulnerabilities.

In this organization, any system containing patient data must have all high-severity vulnerabilities patched within seven days, and no more than one medium-severity vulnerability may remain open at any time. If these limits are exceeded, the issue must be escalated immediately. The organization's low appetite establishes the strategic stance, and the tolerance thresholds guide operational decision-making to remain consistent with that stance.

## Legal, Regulatory, and Contractual Requirements

Stimulus imposed by entities external to the organization typically takes the form of laws, regulations, contractual provisions, professional standards, and other requirements. Often, it is simply enough for laws and regulations to be in place, or for a company to formally accept professional standards for these requirements to be imposed on an organization. Sometimes, however, governance is also imposed as part of contractual requirements between organizations. Including governance requirements in contracts, even if an organization is not otherwise required to meet those requirements, makes them legally enforceable. In any event, organizations are required to fulfill their obligations imposed by these external governance sources.

Additionally, laws, regulations, and other governance sources often conflict with or even supplement each other. For example, one regulation may require a specific level of protection for sensitive data, and another law or regulation may require additional layers of protection based on the characteristics of the data, the organization, or the industry. For example, privacy data and healthcare data are often regulated by multiple sources of governance. In this event, the organization must implement internal policies and procedures to fulfill the requirements of all governance imposed on it. Even in cases where industry standards, such as those imposed by the Payment Card Industry Data Security Standard (PCI DSS), are in place, organizations must fulfill the requirements imposed on them if they have agreed to do so through contract or by virtue of their industry. In this example, organizations aren't legally required to comply with this standard; however, by virtue of the fact that they process credit card transactions, they are required by the credit card industry and can be censured or banned from processing transactions by the credit card companies if they do not comply with the requirements.

Compliance with legal and regulatory requirements is a critical factor in most organizations, and many of these requirements also impose risk management requirements, so risk management is often dictated, to a degree, by governance. In fact, many laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the EU AI Act, require a formalized risk management program. Risk governance frameworks, such as the NIST Risk Management Framework, also require formalized risk management. These frameworks can also be included in any other laws, regulations, contracts, or other governance requirements imposed on an organization.

Multinational organizations must be aware of data sovereignty, residency, and data transfer requirements. *Extraterritorial laws*, including the European General Data Protection Regulation (GDPR) and the EU AI Act, are laws that impose requirements on non-EU organizations that store or process data about European persons.

## Professional Ethics of Risk Management

Most organizations, particularly professional ones, have requirements for a code of conduct or professional ethics, especially in the fields of cybersecurity and risk management. These codes of ethics govern the behavior of professionals, ensuring they maintain high standards of professional conduct and ethics. Most of the industry-recognized professional certifications also require adherence to a code of ethics, and ISACA is no exception.

ISACA's Code of Professional Ethics can be found at `https://www.isaca.org/code-of-professional-ethics` and applies to all organizational members and

certification holders. ISACA also implements procedures for filing complaints against professionals bound to uphold those ethical standards in the event they fail to do so. The ISACA Code of Professional Ethics (paraphrased here) includes provisions for the following:

1. Supporting and complying with standards and procedures for governance and management of information systems and technology
2. Performing duties professionally, with objectivity, due diligence, and care, as required by professional standards
3. Conducting activities in a lawful manner and maintaining the high standards of conduct and character required by the profession and ISACA
4. Ensuring privacy and confidentiality of sensitive information obtained in the course of professional duties
5. Maintaining competency in the professional field
6. Full disclosure and impartiality regarding the results of work performed to ensure that the results of that work are not distorted
7. Supporting professional education in the areas of governance and management of enterprise information systems and technology, including auditing, controls, security, and risk management

# Summary

Governance guides the conduct of an organization in terms of legal and ethical behavior. It can originate from external and internal sources. External governance is imposed through laws, regulations, professional standards, risk frameworks, and contractual requirements, while internal governance arises from the organization's own policies and procedures. The organization's mission, goals, and objectives must reflect and support these governance requirements.

Senior management establishes the organization's risk appetite and tolerance. Risk capacity represents the maximum loss an organization can sustain without threatening its survival. Risk appetite refers to the amount of risk an organization is willing to accept in pursuit of its mission, while risk tolerance defines how much deviation from that appetite is acceptable for specific ventures. Mission, goals, and objectives are typically set at the strategic, long-term level.

Organizational structure influences the ability to manage risk by shaping risk culture, appetite, tolerance, and resilience. Business units and their underlying processes must address both business and IT risk at the process level. Each business process contributes to the organization's overall risk and is managed by a designated risk owner, who is accountable for the risks within their domain. An enterprise risk management (ERM) strategy must address risks at all levels—lower, middle, and higher tiers—with risk governance providing direction for the ERM program.

An organization's risk culture reflects how it perceives and responds to risk, influenced by leadership and governance. Organizational policies form part of internal governance, expressing management philosophy, culture, and leadership directives, and should align with external governance obligations.

Organizational assets encompass everything of value, including facilities, equipment, personnel, and information. Asset management includes the processes for inventorying, classifying, using, and disposing of these assets. The three lines of defense in enterprise risk management are operational management, risk and compliance management, and internal auditing.

The risk profile provides detailed information on an asset and how its characteristics contribute to, mitigate, or influence the associated risk. This profile is used to manage risk effectively. Governance may be mandated by laws, regulations, and contracts, which are legally binding, while codes of conduct and professional ethics guide the behavior of risk management professionals.

# Exam Essentials

**Understand how and why governance is essential.** Governance represents management's control of, and visibility into, essential organizational activities. Governance consists of policies, standards, guidelines, and controls, with measurements and readouts periodically issued to management for their review.

**Understand the underlying principles of the three lines model.** The three lines of defense are operations, risk and compliance, and internal audit. Each must be organizationally independent of the others. Risk and compliance conducts risk assessments and establishes policies and controls that are operated by operations. Internal audit periodically examines controls and processes to ensure they are effective.

**Understand the relationships between policies, standards, guidelines, processes, and procedures.** Policies outline the expected behavior and characteristics of staff, as well as the processes and systems in place. Standards define how policies must be implemented and executed. Guidelines serve as non-mandatory suggestions for implementing policy. Processes are collections of one or more procedures. Procedures are step-by-step instructions for performing a task.

**Recognize that asset management is a cornerstone activity essential for other processes.** Asset management is essential for the integrity of several key processes, including change management, configuration management, vulnerability management, and incident response.

**Know standard governance frameworks.** The most well-known IT governance frameworks include ISACA Risk IT, NIST Risk Management Framework (RMF), COSO ERM, and ISO 31000.

**Understand the relationships between risk appetite, risk tolerance, and risk capacity.** Risk appetite is, in effect, how much risk an organization is willing to deal with in any given endeavor. Risk tolerance, on the other hand, is the acceptable level of deviation in risk for a particular endeavor or business pursuit. Risk capacity refers to the amount of loss an organization can incur without significantly impacting its ability to continue operating.

# Review Questions

The following questions are designed to test your understanding of this chapter's material. For information on how to obtain additional questions, see this book's Introduction. Answers can be found at the end of this chapter.

1. An organization is subject to healthcare regulations that govern the protection requirements of individual health data. Which of the following describes this type of governance?
   - **A.** External
   - **B.** Internal
   - **C.** Regulatory
   - **D.** Professional
2. Your company handles credit card transaction processing as part of its business processes. Which of the following best describes the source and type of governance it may incur because of these business processes?
   - **A.** Internal, policies and procedures
   - **B.** External, industry standards
   - **C.** External, laws and regulations
   - **D.** Internal, industry standards
3. Your organization is structured into various departments, and each of these has its own activities that support the mission, goals, and objectives of the organization. These activities are composed at a high level and include various tasks to support the various business units. Which of the following best describes these activities?
   - **A.** Operational management
   - **B.** Organizational strategy
   - **C.** Business processes
   - **D.** Risk management functions
4. An organizational culture that is averse to risk and change is more likely to have which of the following in terms of risk appetite and tolerance?
   - **A.** High risk appetite, low risk tolerance
   - **B.** Low risk appetite, high risk tolerance
   - **C.** Low risk appetite, low risk tolerance
   - **D.** High risk appetite, high risk tolerance
5. Which of the following roles is the lowest level of responsibility in terms of risk ownership for a business process or unit?
   - **A.** Organizational CEO or president
   - **B.** VP for risk management
   - **C.** Risk practitioner
   - **D.** Business process owner

6. Which of the following is the level of variation or deviance an organization is willing to accept for a particular business venture?
   - **A.** Risk appetite
   - **B.** Risk tolerance
   - **C.** Risk acceptance
   - **D.** Risk capacity

7. A small business unit in the production department is incurring risk for one of its lower-level business processes. Although this risk is focused on the business process and not at the organizational level, it must be accounted for in the overall organizational risk assessment. At what level should this risk be considered?
   - **A.** Organizational risk
   - **B.** Operational risk
   - **C.** Strategic risk
   - **D.** Tactical risk

8. An organization needs to establish its internal risk management program, which begins with risk governance. Which of the following should the organization create first?
   - **A.** Risk strategy
   - **B.** Risk management policy
   - **C.** Risk assessment procedure
   - **D.** Risk management methodology

9. Which of the following describes why the organization exists?
   - **A.** Organizational mission statement
   - **B.** Organizational strategy
   - **C.** External governance
   - **D.** Organizational policy

10. Which of the following activities is considered foundational, without which other management activities, such as vulnerability management, incident management, and data security, could not be accomplished?
    - **A.** Configuration management
    - **B.** Risk management
    - **C.** Asset management
    - **D.** Financial management

**11.** A corporate policy document has a statement that reads, "For critical business processes, the organization permits no more than a low residual risk level, defined as maintaining system availability above 99.5%, preventing any unauthorized access events, and resolving identified high-severity vulnerabilities within 15 days." What type of statement is this?

**A.** Risk culture statement

**B.** Risk capacity statement

**C.** Risk tolerance statement

**D.** Risk appetite statement

**12.** Which of the following requires that a risk practitioner perform duties professionally, with due diligence and care, as required by professional standards?

**A.** Risk IT Framework

**B.** NIST Risk Management Framework

**C.** ISACA Code of Professional Ethics

**D.** Laws and regulations

**13.** A risk manager is analyzing a risk item and has determined that the organization may not survive if the risk is realized. Which of the following must the risk manager consider to make this determination?

**A.** Risk awareness

**B.** Risk capacity

**C.** Risk tolerance

**D.** Risk appetite

**14.** The organization's legal counsel is considering the prospect of real estate prices, including office space leasing costs, increasing significantly in the next five years. What level of risk management should be used to manage this risk?

**A.** Asset

**B.** ERM

**C.** Program

**D.** Market

**15.** All of the following are factors that influence an organization's culture, except:

**A.** Published values

**B.** Policies

**C.** Leadership behavior

**D.** Behavioral norms

16. Which of the following types of organizations is most likely to have a high risk appetite and a high risk tolerance?
    - **A.** Insurance company
    - **B.** Adult beverage producer
    - **C.** Computer manufacturer
    - **D.** AI agent software developer
17. How frequently should an organization review its cybersecurity policies?
    - **A.** Annually
    - **B.** Monthly
    - **C.** Whenever a breach occurs
    - **D.** Every five years
18. A new cybersecurity leader is assessing an organization's risk governance documents and records and has been unable to find any written statements on risk appetite and risk tolerance. How can historic risk appetite and risk tolerance be identified in such a case?
    - **A.** Interview business leaders
    - **B.** Examine incident management records
    - **C.** Examine risk treatment records
    - **D.** Review recent penetration test results
19. All of the following are risk management frameworks, except:
    - **A.** NIST SP 800-37
    - **B.** NIST SP 800-53
    - **C.** COSO ERM
    - **D.** ISO 31000
20. A cybersecurity consultant has observed an organization where its cybersecurity department enacts policies and controls, corporate IT implements these controls, and internal audit assesses the effectiveness of these controls. Which model has the consultant observed?
    - **A.** Deming cycle
    - **B.** Enterprise risk management
    - **C.** Systems development lifecycle
    - **D.** Three lines model

# Answers to Review Questions

1. A. Laws and regulations are a form of external governance. They can also be considered as external inputs to an organization's governance program. Other examples of external inputs include market conditions, customer requirements, and supplier availability. Internal inputs include culture and policy.

2. B. This describes an external source of governance in the form of industry standards, specifically the Payment Card Industry Data Security Standard (PCI DSS).

3. C. Business processes are the activities that support the organizational mission and can be broad or broken down into detailed activities and tasks. Business processes often involve direct human activity, although IT automation enables autonomous business processes, such as the online activation of a new email account.

4. C. A risk-averse organization is likely to have both a low risk appetite and a low risk tolerance. Risk appetite is how much risk an organization is willing to deal with in any given situation, while risk tolerance is the acceptable deviation from risk appetite for a particular matter.

5. D. Although various levels of organizational management may be responsible and accountable for risk, the lowest level of risk ownership for a business process or unit is the business process owner.

6. B. Risk tolerance is the amount of variation or deviation an organization is willing to accept from its risk appetite that a particular business venture may incur. Risk appetite is the amount of risk an organization is willing to undertake. Risk capacity is the amount of loss that an organization can incur while being able to continue operations. Risk acceptance is one of four risk treatment options (the others being mitigate, transfer, and avoid).

7. D. Tactical risks are those encountered by smaller production sections—those that carry out the day-to-day work of the organization. A lower-level business process may be considered to have a tactical risk. Strategic and organizational risks are broad and may affect multiple departments or business units. Operational risks are related to ongoing, internal business operations.

8. A. The risk strategy for the organization should be created first because it provides long-term direction for the risk management program. The risk management strategy also supports external governance. Policies and procedures are subsequently created to support the strategy and implement external governance.

9. A. The organization develops an organizational mission statement to describe its overall purpose, which is its primary reason for existence.

10. C. Asset management is one of the foundational activities on which other activities depend (vulnerability management, configuration management, and so on) because assets must be inventoried and accounted for first.

11. C. A typical risk tolerance statement describes context-specific parameters that represent thresholds that would trigger escalations if exceeded.

12. C. The ISACA Code of Professional Ethics establishes requirements for ethical conduct and behavior that all certified professionals must adhere to, including the requirement to perform all duties professionally, with due diligence and care, as required by professional standards.

13. B. Risk capacity refers to the amount of loss an organization can incur without jeopardizing its ongoing operations.

14. B. A risk matter, such as macroeconomic risk, is generally managed by an organization's enterprise risk management (ERM) program.

**15.** B. Of the available choices, an organization's policies are the least likely to influence an organization's culture.

**16.** D. Of the available choices, the AI agent software developer is most likely to have a high risk appetite and high risk tolerance. The other organizations have more regulations and market reputation to consider, which reduces their risk appetite and tolerance.

**17.** A. The best practice for reviewing policies, including cybersecurity policies, is annually. Organizations should also review their policies when relevant regulations or technologies change, or when business conditions change.

**18.** C. In the absence of a formal, written risk appetite and risk tolerance, the best way to discern historic risk appetite and tolerance is to review the past few years' worth of risk treatment records. This will help the cyber leader better understand what management was willing to accept, versus what management required be mitigated, transferred, or avoided.

**19.** B. NIST SP 800-53 is a controls framework for U.S. government agencies and contractor organizations. The others are risk management frameworks.

**20.** D. The consultant observed the three lines model, also known as the three lines of defense model, in which key responsibilities are divided among three departments in a checks-and-balances model. The Deming Cycle is a lifecycle process. Enterprise risk management is those procedures and records concerning organization-wide risks of all types. The systems development lifecycle is a set of processes to implement a new system.