Chapter 1

Privacy Governance

This chapter covers CDPSE Domain 1, "Privacy Governance," specifically the "Privacy Governance" subdomain.

This chapter covers these job practice elements:

✔ *A—PRIVACY GOVERNANCE*

1. *Personal Information*
2. *Privacy Principles (e.g., Privacy by Design, Consent, Transparency)*
3. *Privacy Laws and Regulations*
4. *Privacy Documentation (e.g., Policies, Guidelines)*

The other subdomain in Domain 1, Privacy Governance, is:

✔ *B—PRIVACY OPERATIONS*—covered in Chapter 2.

The CDPSE Task Statements relevant to this domain are:

1. *Identify internal and external requirements to develop and maintain the organization's privacy programs.*
6. *Contribute to the integration of privacy principles (e.g., privacy by design) in the development of procedures and operational manuals for organizational needs.*
7. *Collaborate with stakeholders to promote privacy principles (e.g., privacy by design) are followed during the design, development, and implementation of systems, applications, and infrastructure.*
17. *Advocate for advancing privacy posture and maturity as it aligns with the organizational objectives.*

The topics in this chapter and in Chapter 2 account for 20% of the CDPSE examination.

COPYRIGHTED MATERIAL

This chapter introduces the foundational concepts of privacy governance, establishing how organizations manage personal information in alignment with legal, regulatory, and business requirements. The chapter begins with governance structures, roles, and accountability models that define oversight and decision-making, including the integration of privacy into enterprise strategy. The chapter then examines the nature of personal information, key privacy principles such as transparency and data minimization, and the legal and regulatory frameworks that shape organizational obligations. It also addresses privacy documentation, including policies, notices, and records that support consistent and compliant operations. Supporting topics such as privacy program strategy, lifecycle management, and the three lines of defense provide additional context on how privacy is operationalized and sustained. Together, these elements form a comprehensive view of how organizations design, implement, and maintain effective privacy governance programs.

While not explicitly a part of the CDPSE job practice, this chapter begins with a comprehensive discussion of governance and the development of a privacy program strategy.

Introduction to Privacy Governance

Privacy governance is a set of established *governance* lifecycle activities that typically focus on several fundamental principles and outcomes, designed to enable management to have a clear understanding of the state of the organization's *privacy* program, its current risks, its direct activities, and its alignment with the organization's business objectives and practices. A goal of the privacy program is to enable the fulfillment of the privacy strategy, which itself will continue to align with the business, business objectives, and evolving regulations. The processes supporting these principles and outcomes include privacy policy, data governance, compliance, risk management, and cybersecurity. Whether the organization has a board of

directors, council members, commissioners, or another top-level governing body, governance begins with establishing top-level strategic objectives that are translated into actions, roles, and responsibilities through policies, processes, procedures, and other activities, cascading downward through each level of the organization.

Privacy is a business issue, and organizations that are not yet properly managing or adequately protecting personal information have a business problem. The reason for this is almost always a lack of understanding and commitment by boards of directors and senior executives. For many, privacy is viewed as a security issue that focuses on tactical data protection problems or on data usage problems, and it's not about protection at all. The challenge is that, due to a lack of awareness or experience with privacy, organizations still struggle to organize, manage, and communicate about privacy successfully at the executive leadership and boardroom levels.

To manage privacy successfully, organizations need to understand that privacy is also a people issue. When people at every level of the organization—from board members to individual contributors—understand the importance of privacy and security in their roles and responsibilities, the organization will be at reduced risk. This reduction in risk or identification of potential privacy or security events results in fewer incidents with less impact on the organization's ongoing reputation and operations.

A privacy program operates as a lifecycle to ensure that governance, controls, and practices progress alongside regulatory, technology, and business changes. A privacy program consists of these components:

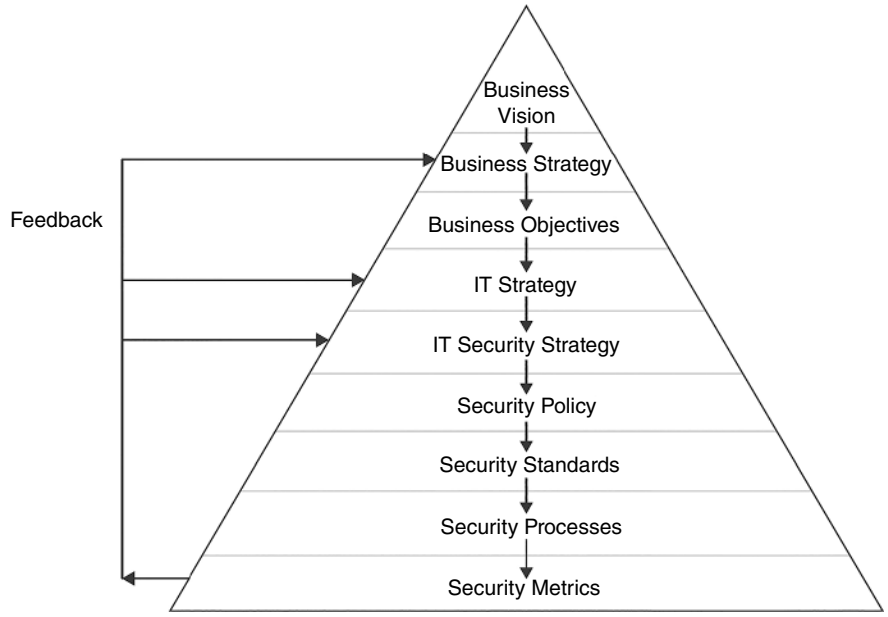
- **Initiation** Establish the foundation of the privacy program by identifying legal, regulatory, and business requirements. Define scope, objectives, stakeholders, and governance structure.
- **Design** Develop policies, standards, processes, and controls that align with privacy principles and organizational objectives. Architect the program to address data lifecycle activities, risk management, and compliance obligations.
- **Implementation** Deploy the designed controls, processes, and technologies across the organization. Assign roles and responsibilities, conduct training, and integrate privacy into business operations and system development.
- **Monitoring** Continuously assess the effectiveness of privacy controls and processes through metrics, audits, and reviews. Identify gaps, incidents, and compliance issues to ensure ongoing alignment with requirements.
- **Continual improvement** Refine and enhance the privacy program based on monitoring results, regulatory changes, and evolving risks. Implement corrective actions and maturity improvements to strengthen governance and operational effectiveness.

A mature privacy program treats this lifecycle as iterative, ensuring sustained alignment with organizational goals, regulatory constraints, and emerging risks.

Because modern privacy practices are heavily influenced by privacy laws such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the California Privacy Rights Act (CPRA), organizations should rely on qualified legal counsel as part of their overall governance process. Including legal counsel helps to ensure that the organization's privacy policies and practices comply with these and other laws.

Think of privacy as having two main components: proper data management and usage and data protection—commonly referred to as cybersecurity, data security, or information security. A privacy program cannot succeed without effective cybersecurity. Further, cybersecurity cannot succeed without a solid foundation in IT and IT operations. IT is the enabler and force multiplier that facilitates business processes that fulfill organizational objectives. Without effective IT governance, privacy and *information security governance* will not reach their full potential. The result might be that the IT bus will travel safely, but to the wrong destination. Figure 1.1 shows how the business vision, strategy, and objectives of privacy and information security governance flow downward through an organization's privacy and IT security strategies, policies, standards, and processes.

FIGURE 1.1 In a governance model, vision flows downward, and reporting and metrics flow upward.



Source: Author.

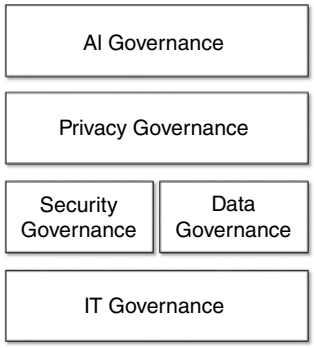
Although the CDPSE certification is not directly tied to IT governance, this implicit dependence of privacy and security governance on IT governance cannot be understated. IT and security professionals specializing in IT governance might be interested in ISACA's Certified Information Security Manager (CISM) and Certified in the Governance of Enterprise IT (CGEIT) certifications, which focus on these domains.

For privacy governance to succeed, organizations also need effective security, data, and IT governance. Figure 1.2 depicts these dependencies. And while outside the scope of this book, AI governance depends on privacy governance because many organizations train their AI systems on personal information.

While IT governance, information security governance, and privacy governance can be separate activities, in many organizations, these activities will closely resemble or rely on one another. Many issues will span IT, security, and privacy governance bodies, and many individuals will participate actively in all three areas. Some organizations integrate IT, information security, and privacy governance into a single set of participants, activities, and business records. The most important thing is for organizations to establish governance programs that effectively achieve formally established business outcomes.

Privacy governance will enable alignment of the organization's privacy program with customer or constituent expectations, applicable regulations, identified risks, and business needs. An objective of *privacy governance* is to provide, from a strategic perspective, assurance of the proper protection and use of personal information, ensuring that required privacy practices align with business practices. These are some of the artifacts and activities that flow out of sound privacy governance:

FIGURE 1.2 Privacy governance relies upon security and data governance, which in turn rely upon IT governance.



Source: Author.

- **Objectives** The desired capabilities or end states, ideally expressed in achievable, measurable terms.
- **Established legal basis** The way the organization can lawfully collect and process personal information about data subjects.
- **Consent** The mechanism through which the organization directly or indirectly obtains permission from data subjects to collect and process their personal information.
- **Strategy** The plan to achieve one or more objectives.
- **Policy** The mission, objectives, and goals of the overall organization that align with constituent expectations and applicable laws.
- **Priorities** The main concerns of the privacy program, which should flow directly from the organization's mission, objectives, and goals. Whatever is most important to the organization should be relevant to privacy and information security.
- **Standards** The technologies, protocols, and practices used by IT that 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 cost-effectively and securely.
- **Processes** The formalized descriptions of repeated business activities that include instructions to applicable personnel. Processes consist of one or more procedures, along with definitions of business records and other facts that help workers understand how things are supposed to be done.
- **Controls** The formal descriptions of critical activities performed to ensure desired outcomes.
- **Program and project management** The ways in which the organization's privacy, security, and IT programs and projects are organized and performed, which should be in a consistent manner that reflects business priorities and supports the business.
- **Metrics/reporting** The formal measurement of processes and controls that management can understand and measure.
- **Review/audit** The formal evaluation of processes and controls to determine their effectiveness.

To the greatest extent possible, privacy governance in an organization should be practiced in the same way the organization approaches cybersecurity, IT, and overall corporate governance. Privacy governance should either mimic organizational, security, and/or IT governance processes or be integrated into corporate, cybersecurity, or IT governance processes.

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

Privacy and Security: Together or Separate?

Should privacy and security be managed separately or together? Although there's no right or wrong answer, know this: privacy cannot succeed without information security. The objectives of a privacy program are to protect and properly handle personal information. The protection part is done by information security, and the proper handling part is solely the domain of privacy.

Privacy needs information security to be successful. Security is a prerequisite to privacy, but privacy adds more: the proper *handling* of information and its *protection*.

This is why privacy and security are discussed hand in hand throughout this chapter and throughout most of this book. Discussing privacy alone, without security, tells only half the story.

The Three Lines of Defense

The *three lines of defense* is a governance framework that clarifies accountability for risk management, control, and assurance across an organization. Responsibilities are separated to ensure that risks to personal information are identified, managed, and independently evaluated. The aspects are as follows:

- **First line: Operations** Business units and teams collect, use, and manage personal information. They implement privacy controls and ensure that day-to-day activities comply with legal and organizational policies and requirements. They own risks associated with their processes and are accountable for properly handling data.
- **Second line: Privacy, Compliance, and Risk Management** These groups establish policies, standards, guidelines, and monitor adherence to requirements. They support the first line by interpreting laws and regulations, advising on privacy risks, and overseeing control effectiveness.
- **Third line: Internal Audit** This group provides independent assurance to senior management and the board of directors by performing audits of governance, risk management, processes, and privacy-related controls.

These three functions are assigned to three different persons or teams that operate independently and collaborate extensively. The three lines of defense model is an implementation of the separation of duties, in which essential functions are divided among multiple parties so that no single party can exert excessive control or suffer from groupthink.

Privacy Governance Influencers

An organization's privacy program must focus on several internal and external events and activities. Privacy professionals recognize that some of these factors can be influenced to some degree, while others are entirely outside the privacy professional's sphere of influence. We must be informed and able to react to these influencers.

Much of the information in information systems concerns people. In both government and business, information systems keep track of property owners, taxpayers, voters, patients, clients, customers, and potential customers. Often, the information retained about people is sensitive—even secretive—and all parties have a vested interest in the adequate protection of that information.

In most situations, transactions between individuals and businesses, governments, and healthcare organizations are considered confidential, not to be disclosed, and to be used only for official business purposes.

When this information migrated from paper to information systems and with advancements in information technology, organizations developed numerous techniques to obtain more value from information about their citizens, patients, customers, and constituents. Abuses of these practices have given rise to privacy laws intended to curb these activities.

Privacy laws are discussed in detail in this section. Note that there are many variances among these laws in the following areas:

- **Definitions of personal information** Privacy laws sometimes provide specific, sometimes vague definitions of which types of data are considered sensitive and which are not. Most laws consider the aggregation of someone's name, along with other items such as financial account numbers, medical records, political affiliation, and more, to be personal information that is to be safeguarded and used within stated guidelines.
- **Data subject rights** Privacy laws define many rights that vary somewhat from one regulation to another. These rights include transparency, limitations on use, adequate protection, correction, and removal.
- **Protection of personal information** Laws require organizations to take measures to ensure the adequate protection of personal information, so that it cannot be accessed, altered, stolen, or destroyed by unauthorized parties.
- **Use of personal information** Laws require transparency regarding the use of personal information, so that persons can be aware of these uses.
- **Notification of breach** Laws require organizations to disclose to affected individuals any instances in which their personal information was improperly accessed, used, or compromised.
- **Jurisdiction** Many privacy laws today are "extraterritorial," meaning they are intended to regulate the activities of organizations located outside political boundaries.

Data privacy and data protection laws are being enacted at a relatively fast pace, reflecting the vast expansion of the collection and use of personal information, abuses and

breaches by organizations that collect and use personal data, and still-developing social norms regarding the definitions and expectations of privacy.

The Imperfect Lexicon of Privacy

As with any profession, privacy and information security have their own specialized vocabulary. In the privacy profession, we use the terms *personal information* and *data subject request*. Is there really a distinction and a valid reason why "personal information" uses the term *information* while "data subject request" uses the term *data*?

In practical terms, *data* consists of raw values, symbols, or observations (such as numbers, text strings, or timestamps) that, on their own, can lack meaning. *Information* is produced when data is organized, processed, or interpreted in context, enabling understanding and supporting decision-making.

This distinction is important in privacy governance because legal and regulatory obligations generally apply to information about identifiable individuals, even though that information is often stored and processed as data within information systems.

Perhaps this is a clue. The remainder of this exercise is left to the reader.

Reasons for Privacy Governance

Whether you attribute the emergence of sweeping data privacy laws to citizen backlash or to a coming of age, organizations everywhere are becoming aware that people's privacy rights matter and that ignoring them can land an organization in hot water. For the most part, organizations are being forced to change their practices, information systems, and sometimes even their business models to align with the new reality: they must be transparent about how they obtain, collect, process, and share personal information.

Governance is management's sharpest tool for getting things done. Regarding privacy laws such as the GDPR, CCPA, and CPRA, organizations have put governance structures in place to oversee the transformation in their business processes and information systems from practices of opaqueness to practices of transparency. In many cases, this transformation meant an about-face on internal practices. Indeed, this has prompted numerous (dare I say, the majority of) organizations to "discover" how they use personal information internally, as though the proverbial foxes have been in charge of the henhouse.

Simply put, privacy governance is all about keeping organizations out of trouble with regulators, outraged citizens, and the courts. Many organizations have shown no desire to change their business models, and many complain that doing so will hurt them financially. Just as the do-not-call lists have curbed the use of unsolicited "robo-calls" in the United States, privacy laws will forever alter business models that mine and monetize personal data behind the dark curtains of organizations' marketing machines.

While the foregoing portrays the darker side of some organizations, many others were already "doing the right thing" regarding transparency in the management of personal data. For them, the new journey to privacy compliance has been less impactful.

Because privacy governance is driven by emerging privacy laws, many organizations have legal counsel in their governance structure as experts on the law and its interpretation. As more privacy laws are enacted and case law begins to emerge, organizations will monitor their development and adjust processes and systems accordingly.

The flexibility and capabilities of information systems make it all too easy for organizations to exceed the implicit or explicit purposes for which personal information is collected and used, leading to potential abuses and overreach. As a privacy professional, you must understand the business's operations regarding data about natural persons, including how it is collected, used, and protected. These four things should be considered when you're building out a privacy governance structure. Still, the type of information the organization uses will drive the priority given to managing data use and protection. Privacy governance, then, is needed to ensure that the organization's data management and protection activities do not lead to incidents that could harm affected persons or the organization itself.

Privacy and Security Governance Activities and Results

Within effective privacy and security governance programs, an organization's senior management team will ensure that information systems necessary to support business operations are adequately protected and that data about natural persons is properly collected, managed, and used. These are some of the activities required to protect personal data and information:

- **Risk management** Management will ensure that risk assessments are performed to identify risks in business processes and information systems. Follow-up actions will be carried out to reduce the risk of system failure and compromise.
- **Process improvement** Management will ensure that key changes are made to business processes to achieve compliance with privacy laws and improve cybersecurity.
- **Event identification** Management will put technologies and processes in place to ensure that privacy and security events and incidents are recognized and acted upon as quickly as possible.
- **Incident response** Management will implement incident response procedures to help prevent incidents, reduce the likelihood and impact of incidents, and improve response to incidents, thereby minimizing their impact on the organization.
- **Improved compliance** Management will ensure that all applicable laws, regulations, standards, and other legal obligations are identified and that activities are carried out to confirm the organization can attain and maintain compliance.
- **Metrics** Management will establish processes to measure key privacy and security events, including subject requests, complaints, incidents, policy changes, violations, audits, and training.

- **Resource management** Management will *monitor* the allocation of staffing, *budget*, and other resources to meet privacy and security objectives.
- **Improved IT governance** Management will implement an effective privacy governance program that will result in better strategic decisions that keep risks at an acceptably low level.

These and other governance activities are carried out through scripted interactions among key business, privacy, security, and IT executives at regular intervals. Meetings will include a discussion of the impact of regulatory changes, alignment with business objectives, the effectiveness of measurements, recent incidents, recent audits, and risk assessments. Other discussions can include changes to the business, recent business results, and anticipated business events, such as mergers or acquisitions.

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

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

Business Alignment

An organization's information privacy program needs to fit in with the rest of the organization. This means that the program needs to align with the organization's highest-level guiding principles, including the following:

- **Mission** Why does the organization exist? Who does it serve, and through what products and services?
- **Goals and objectives** What achievements does the organization want to accomplish, and when does it want to achieve them?
- **Strategy** What are the activities that need to take place so that the organization's goals and objectives can be fulfilled?

To be business aligned, privacy and security professionals should be aware of several characteristics of the organization, including the following:

- **Business model and processes** This includes the organization's data flows (particularly flows of personal information), its use of information systems, and its sources of revenue.
- **Sources and uses of personal information** At the core of a privacy program, it's vital that all sanctioned and unsanctioned uses of personal information are understood, documented, rationalized, and managed.
- **Culture** This includes how personnel in the organization work, think, and relate to each other. Of utmost importance is the cultural attitude toward the treatment of personal information.

- **Asset value** This includes information the organization uses to operate. This often includes intellectual property such as designs and source code, as well as sensitive information related not only to the organization's personnel but also to its customers, information-processing infrastructure, and service functions.
- **Risk tolerance** Risk tolerance for the organization's privacy and information security programs needs to align with the organization's overall tolerance for risk.
- **Legal obligations** What external laws and regulations govern what the organization does and how it operates? These laws and regulations include the GLBA, GDPR, CCPA, CPRA, and HIPAA. Also, contractual obligations with other parties often shape the organization's behaviors and practices.
- **Market conditions** How competitive is the marketplace in which the organization operates? What strengths and weaknesses does the organization have in comparison with its competitors? How does the organization want its privacy and security to be differentiated from those of its competitors?
- **Privacy law enforcement** Are regulators and other authorities actively enforcing privacy laws and regulations, or are those laws "paper tigers" that stand unenforced. Organizations are generally reluctant to invest in changing business models, business processes, and information systems to comply with laws that might not be enforced.

Goals and Objectives

An organization's goals and objectives specify the activities that are to take place in support of the organization's overall strategy. Goals and objectives are typically statements in the form of imperatives that describe the development or improvement of business capabilities. For instance, goals and objectives can be related to increases in capacity, improvements in quality, or the development of entirely new capabilities. Goals and objectives further the organization's mission, helping it to continue to attract new customers or constituents, increase market share, and increase revenue and/or profitability.

Risk Appetite, Tolerance, and Capacity

Each organization has a particular "appetite" for risk, though few have documented it. ISACA defines *risk appetite* as "the level of risk that an organization is willing to accept while in pursuit of its mission, strategy, and objectives, and before action is needed to treat the risk."

Risk tolerance is related to risk appetite. ISACA defines *risk tolerance* as "the acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives."

Risk capacity is related to risk appetite. ISACA defines *risk capacity* as "the objective amount of loss that an organization can tolerate without its continued existence being called into question."

Generally, only highly risk-averse organizations such as banks, insurance companies, and public utilities will document and define risk appetite in concrete terms. Other organizations

are more tolerant of risk and make individual risk decisions based on gut feeling or qualitative risk analysis. However, due to increased regulation, customer influence, and mandates, many organizations are finding it necessary to document and articulate their risk posture and appetite. This is an emerging trend in the marketplace, but it is still relatively new to many organizations.

In a properly functioning risk management program, the chief information security officer (CISO) is rarely the person who makes a risk-treatment decision or is accountable for it. Instead, the CISO is a *facilitator* for risk discussions that eventually lead to risk treatment decisions. The only time the CISO would be the accountable party is when risk treatment decisions directly affect the risk management program itself, such as in selecting a governance, risk, and compliance (GRC) tool for managing and reporting on risk.

The data privacy officer (DPO) plays a role in privacy-related risk decisions. Like the CISO, the DPO is a domain expert and guides the business toward decisions that align with applicable laws, internal policies, and the expectations of its affected constituents. Generally, it is business leaders who will make those decisions.

Privacy Governance Frameworks

It is unnecessary to build a privacy governance framework from scratch when industry-standard privacy frameworks are available for the privacy leader to consider. These frameworks include:

- NIST Privacy Framework
- ISO/IEC 27701

These frameworks are described in detail in Chapter 4.

Privacy Strategy Development

Among business, technology, privacy, and security professionals, there are many different ideas about the meaning of *strategy*, *strategic planning*, and the techniques used to develop one, which can result in general confusion. Although a specific strategy itself can be complex, the concept of a strategy is quite simple. A *strategy* can be defined as *a plan to achieve an objective*.

The effort to build a strategy requires more than saying those six words. Again, however, the idea is not complicated. The concept is this: understand where you are now and where you want to be. The strategy is the path you must follow to get from where you are (current state) to where you want to be (strategic objective).

The remainder of this section explores strategy development in more detail.

This section discusses privacy and security together because privacy depends on security for its information-protection capabilities.

Strategy Objectives

As stated earlier in this section, a strategy is a plan to achieve an objective. The objective (or objectives) is the desired future state of the organization's privacy and security posture and risk level.

There are, in addition, objectives *of* a strategy:

- **Strategic alignment** The desired future state, and the strategy to get there, must align with the organization and *its* strategy and objectives.
- **Effective risk management** Privacy and security programs must include a risk management policy, processes, and procedures. Without risk management, decisions are made blindly without regard to their consequences or level of risk.
- **Value delivery** The desired future state of a privacy or security program should focus on continual improvement and increased efficiency. No organization has unlimited funds for privacy and security; instead, organizations need to reduce the right risks for the lowest reasonable cost.
- **Resource optimization** Similar to value delivery, strategic goals should efficiently utilize available resources. Among other things, this means having only the necessary staff and tools required to meet strategic objectives.
- **Performance measurement** While strategic objectives need to be SMART, the ongoing privacy and privacy-related business operations should themselves be measurable, enabling management to drive continual improvement.
- **Assurance process integration** Organizations typically operate one or more separate assurance processes in silos that are not integrated. An effective strategy would work to break down these silos and consolidate assurance processes, reducing hidden risks.

All of these should be developed in a way that makes them measurable. This is why these six topics were discussed earlier when discussing governance metrics. These components were made to fit together in this way.

Risk Objectives

A vital part of strategy development is determining desired risk levels. One input to strategy development is understanding the current level of risk, and the desired future state can also have a level of risk associated with it.

It is quite difficult to quantify risk, even for the most mature organizations. Getting risk to a reasonable "high-medium-low" is simpler, though less straightforward, and difficult

to do consistently across an organization. In specific instances, the costs of individual controls can be known, and the costs of theoretical losses can be estimated, but doing so across an entire risk-control framework is tedious and uncertain because the probabilities of threat-event occurrence amount to little more than guesswork.

A key part of a privacy strategy might well be reducing risk (it could also be cost reduction or compliance improvement). When this is the case, the strategist will need to employ a method for determining reasonable, credible before-and-after risk levels. For the sake of consistency, a better approach would be to use a methodology—however specific or general—that aligns with other risk-related strategies and discussions.

Strategy Resources

A strategy describes the process by which goals and objectives are to be met. Before an organization can develop a privacy and security strategy, it must first understand what privacy and security measures are currently in place. Existing resources paint a picture of an organization's current capabilities, including behaviors, skills, practices, and posture. The gap between the current and future states can then be filled through technologies, skills, policies, or practices.

Two types of inputs must be considered: those that will influence the development of strategic objectives and those that define the current state of privacy and security programs and their protective controls. The following inputs must be considered before objectives are developed:

- Risk assessments
- Threat assessments

When suitable risk and threat assessments have been completed, a privacy or security strategist can develop strategic objectives, or, if objectives have already been created, determine whether they will satisfactorily address the risks and threats identified in those assessments.

Privacy and security strategists can examine additional inputs to better understand the workings of the current privacy and security program. Many of these activities are more security-centric than privacy-centric, because a successful privacy program requires an effective security program as a foundation. These activities include the following:

- **Program charter** The organization might have a privacy program charter that defines a strategy, roles and responsibilities, objectives, or other matters.
- **Risk assessments** A risk assessment can reveal privacy and security risks within the organization. This helps the strategist understand threat scenarios, their estimated impacts, and their frequency. Risk assessment results provide the strategist with valuable

information on the types of resources required to bring risks to acceptable levels. This is vital for developing and validating strategic objectives.

- **Threat assessments** A threat assessment provides the strategist with information on the types of threats most likely to affect the organization, regardless of the effectiveness of controls. A threat assessment provides an additional perspective on risk, because it focuses on external threats and threat scenarios, regardless of the presence or effectiveness of preventive or detective controls.

A threat assessment is an essential element of strategy development. Without a threat assessment, strategic objectives can fail to address important threats. This would result in a privacy or security strategy that would not adequately protect the organization.

- **Vulnerability assessments** A vulnerability assessment helps the strategist better understand the current privacy and security postures of the organization's processes and infrastructure. The vulnerability assessment can target personnel, business processes, network devices, appliances, operating systems, subsystems such as web servers and database management systems, and applications, or any suitable combination thereof.
- **Maturity assessments** A maturity assessment provides the strategist with valuable information about the maturity of business processes. A strategist will better understand whether processes are orderly, organized, consistent, measured, examined, and periodically improved.
- **Audits** Internal and external audits can tell the strategist quite a bit about the state of the organization's privacy and security programs. A careful examination of audit findings can potentially provide significant details on regulatory compliance, control effectiveness, vulnerabilities, disaster preparedness, or other aspects of the program—depending on the objectives of those audits.

The topic of audits is discussed in considerable detail in the book, *CISA Study Guide* (Wiley Publishing), by this author.

- **Policies** An organization's privacy and security policies, as well as its practices regarding them, can say a great deal about its desired current state. Privacy and security policies can be thought of as an organization's internal laws and regulations regarding the protection and proper use of personal information and other assets. Examining the current privacy and security policy can reveal a lot about the behaviors required within the organization. Assessments, discussed earlier in this list, help a strategist understand the organization's compliance with its policies.

Many organizations align their privacy and security policies with the privacy and security control frameworks they have adopted.

- **Standards** Privacy and security *standards* describe, in detail, the methods, techniques, technologies, specifications, brands, and configurations to be used throughout the organization. As with privacy and security policies, privacy and security managers must understand the breadth of coverage, strictness, compliance, and last review and update of the organization's standards. These all indicate the extent to which an organization's privacy and security standards are used, if at all.
- **Guidelines** The very presence of current, actionable *guidelines* can signal a higher-than-average maturity. Most organizations don't get beyond creating policies and standards, so the presence of proper guidelines means the organization might have (or had in the past) sufficient resources or prioritization to make documenting policy guidance important enough to do. By their very nature, guidelines are typically written for personnel who need assistance with policy and standard compliance.
- **Processes and procedures** An organization's *processes* and *procedures* might speak volumes about its level of discipline, consistency, risk tolerance, and the maturity of not only its privacy and security programs but also of IT and the business in general. Like other types of documents discussed in this section, the relevance, accuracy, and thoroughness of process and procedure documents are indicators of maturity and commitment to robust privacy and security programs. Strategists need to confirm whether processes and procedures are actually followed or merely written artifacts.
- **Architecture** An organization's documentation of systems, networks, data flows, and other aspects of its environment provides privacy and security strategists with valuable information about how the organization has implemented its information systems and the business processes it supports. Documentation in the form of architecture diagrams is as important as written policies, standards, guidelines, and other artifacts. The strategist needs to determine whether the organization's architecture supports the organization's goals, objectives, and operations.
- **Controls** The strategist should review artifacts and interview personnel to determine whether specific controls are in place. The presence of documentation alone might not indicate whether controls are being carried out or merely more shelfware. Interviewing personnel and observing controls in action are better ways to determine whether controls are in place. Internal and external audits, discussed earlier in the "Audits" item, are another way to understand control effectiveness. A strategist will also need to understand whether the controls in place are part of a control framework such as ISO/IEC 27701, ISO/IEC 27001, NIST 800-53, CIS CSC, GLBA, HIPAA, or PCI DSS.
- **Skills and knowledge** An inventory of skills provides the strategist with an idea of what staff members can accomplish. Understanding skills at all these levels helps the strategist identify the types of work the current staff can perform, where minor skills

gaps exist, and where the strategist might recommend additional staff through hiring, contracting, or professional services. A key consideration is the potential for a major shift in practices and technologies. A good example is when the organization has been "playing it loose" with personal information and has not yet adopted data governance and data management practices required in modern privacy programs. If the staff lacks knowledge of these practices, the organization will struggle to implement them to comply with applicable privacy regulations.

- **Metrics** Properly established metrics will serve as a guide for the long-term effectiveness of privacy and security controls and processes. Evaluating such metrics helps the strategist understand what works well and where there are opportunities for improvement. The strategist can then design end states with more certainty and confidence than if metrics didn't exist.
- **Assets** The strategist needs to determine whether the organization has formal asset management practices and records to track its hardware (including virtual machines and other virtual assets), software, and data. Asset management is a key activity for both privacy and security programs, as information security professionals often say, "You cannot protect what you cannot find."
- **Risk register** The presence of a risk register can give the strategist a great deal of insight into risk management and risk analysis activities within the organization. Depending on the detail available in the risk ledger, a strategist might be able to discern the scope, frequency, quality, and maturity of risk assessments; the presence of a risk management and risk treatment process; and whether there are records of incidents.
- **Risk treatment decision records** When available, risk treatment records reveal which issues warranted attention, discussion, and decision-making. Coupled with the risk ledger, this information can provide a record of issues addressed by the organization's risk management process.
- **Insurance** The privacy or security strategist might want to know whether the organization has cybersecurity insurance or any general insurance policy that covers some types of cyber events and incidents. As important as having cyber insurance is, equally important is the reason the organization purchased it: compliance requirements, customer requirements, prior incidents, or a risk treatment decision. It is vitally important to understand the terms of any cyber-insurance policy. While the amounts of benefits are important, the most important aspects of a cyber-insurance policy are its terms, conditions, and exclusions.
- **Data management practices** The strategist needs to understand whether the organization has formal data management practices, including but not limited to a data classification policy, an internal privacy policy, and whether any tooling exists (such as DLP in its many forms) to provide visibility and control over the movement and use of personal information and other sensitive data.
- **Critical data** Privacy and security strategists need to understand the nature and use of an organization's critical data. But first, it's important to understand the term *critical*.

There are at least three common uses of the term when associated with data: operational criticality, highly sensitive (including personal information), and market criticality (including intellectual property and other competitive data).

- **Business impact analysis** While a business impact analysis (BIA) identifies an organization's business processes, the interdependencies between processes, the resources required for process operation, and the impact on the organization if any business process is incapacitated for a time for any reason, the BIA is also useful for privacy and security professionals aside from business continuity purposes, by giving the security strategist a better idea of which business processes and systems warrant the greatest protection.

The presence of a recent BIA provides a strong indication of the organization's maturity, as it signals an intention to protect its most critical processes from disaster scenarios. Consequently, the absence of a BIA suggests that the organization does not consider BCDR to be of strategic importance.

- **Privacy and security incident logs** Privacy and security incident logs provide the strategist with a history of incidents that have occurred in the organization. Depending on the information captured in the incident log, the strategist might be able to discern the maturity of the organization's privacy and security programs, especially its incident response program. The absence of incident logs is a strong indicator of the absence of an incident response process.
- **Outsourced services** The degree to which any particular organization has outsourced its business applications to the cloud is not the concern. Instead, what's important is the level of due care exercised in the outsourcing process, namely, whether a formal third-party risk management (TPRM) program is in place.
- **Culture** The *culture* of an organization can tell the strategist a lot about the state of privacy and security. Many people mistakenly believe that privacy and information security are all about technology. While technology is part of privacy and security, people are the most important aspect of a privacy and security program. No amount of technology can adequately compensate for an incorrect attitude and understanding regarding the protection of an organization's information assets, or for the mishandling of personal information. People are absolutely key.

When considering an organization's culture, the strategist needs to rely more on the organization's *actual operations* than on its statements of culture and values. The actual organizational culture might not align with the organization's claims.

- ***Maturity*** The characteristics of privacy and security management programs discussed in this list all contribute to the overall maturity of the organization's program. By itself, the program's maturity level doesn't tell the strategist anything about its details. But the strategist's observations of the program will provide a visceral sense of its maturity.
- **Risk appetite** Undocumented in most organizations, risk appetite can be discerned from the record of risk treatment decisions and from observations of an organization's executive culture. Even then, however, the attitude and culture of risk appetite might differ from an organization's actual practices.

Privacy Program Strategy Development

After the strategist has performed risk and threat assessments and carefully reviewed the state of privacy and security *programs* by examining artifacts, the strategist can develop strategic objectives. Strategic objectives will fall into one or more of these categories:

- Improvements in data management processes
- Improvements in protective controls
- Improvements in incident visibility
- Improvements in incident response
- Reductions in risk, including compliance risk
- Reductions in cost
- Increased resiliency of key business systems

These categories all contribute to strategic improvements in an organization's privacy and security programs. Depending on the current and desired future state of privacy and security, objectives might represent large projects or groups of projects implemented over several years to develop broad new capabilities, or they might be smaller projects focused on improving existing capabilities.

Here are some examples of broad, sweeping objectives for developing new privacy and security capabilities:

- Define and implement a data loss prevention (DLP) system to provide visibility and control over the movement of personal information.
- Define and implement a SIEM system to provide visibility into privacy, security, and operational events.
- Define and implement a privacy incident response program.
- Define and implement a security awareness learning program.

Here are examples of objectives for improving existing capabilities:

- Integrate vulnerability management and GRC systems.
- Link privacy awareness and access management programs so that staff members must complete privacy awareness training to retain access to systems containing personal information.

Once one or more objectives have been identified, the strategist will undertake several activities required to meet them. These activities are explained in the remainder of this section.

The strategist must consider many inputs before developing objectives and strategies to achieve them. These inputs serve a critical purpose: to help the strategist understand the organization's current state. The process of developing and implementing a strategy is not possible without understanding the starting point. These are discussed in the previous section, "Strategy Resources."

Gap Analysis

When developing a privacy and security strategy and objectives, privacy and security professionals often spend too much time focusing on end goals and too little on the current state of the organization's privacy and security program. Without sufficient knowledge of the current state, however, the strategist will find that accomplishing objectives will be more difficult and achieving success less certain.

A gap analysis helps the strategist understand missing capabilities and augment existing capabilities to achieve the desired end state. When performing a gap analysis, the strategist examines the present condition of processes, technologies, and people.

A gap analysis focuses on several aspects of a privacy or security program, including items from the prior "Strategy Resources" section.

When examining all of this and other information about an organization's privacy and security programs, the strategist should bring the appropriate measure of skepticism. There is much to know about what information is found, but the absence of information can speak volumes as well. Here are some considerations:

- **Absence of evidence is not evidence of absence** This time-honored adage applies to artifacts in any program. For instance, a sparse or nonexistent incident log might be an indication of several things: the organization might not have the required visibility to know when an incident has taken place, the organization's staff might not be trained in the recognition of incidents, or the organization might be watching only for "black swan" events and might be missing routine incidents.
- **Freshness, usefulness, and window dressing** When it comes to policy, process, and procedure documentation, it is important to determine whether documents are created for appearances only (in which case they might be well-kept secrets except to their owners) or widely known and utilized. A look at these documents' revision histories tells part of the story, while interviewing the right personnel completes the picture by revealing how well the documents' existence is made known and whether they are really used.
- **Scope, turf, and politics** In larger organizations, privacy and security managers need to understand current and historical practices regarding roles and responsibilities for privacy, security, and related activities. For example, records for a global security

program might reflect only what is occurring in the Americas, even though there is no written record to the contrary.

- **Reading between the lines** Depending on the organization's culture and the ethics of current or prior privacy and security personnel, records might not accurately reflect goings-on in the program. In other words, there might be overemphasis, underemphasis, distortions, or simply "look-the-other-way" situations that might result in records being incomplete.
- **Off the books** For various reasons, certain activities and proceedings in a privacy or security program might not be documented. For example, certain incidents might conveniently be absent from the incident log—otherwise, external auditors might catch the scent and go on a foxhunt, causing all manner of unpleasantness.
- **Regulatory requirements** When examining each aspect of a privacy or security program, the program's manager needs to ask one important question: is that activity included because it is required by regulations (with hell and fury from regulators if absent) or because the organization is managing risk and attempting to reduce the probability and/or impact of potential threats?

A common approach to determining the future state in a gap analysis is to determine the current maturity of a process or technology and compare that to the desired maturity level. Continue reading in the next section for a discussion on maturity levels.

Strengths, Weaknesses, Opportunities, and Threats Analysis

A Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis is a tool used in support of strategic planning. SWOT involves introspective analysis, where the strategist asks questions about the four components of the object of study:

- **Strengths** What characteristics of the business give it an advantage over others?
- **Weaknesses** What characteristics of the business put it at a disadvantage?
- **Opportunities** What elements in the environment could the business use to its advantage?
- **Threats** What elements in the environment threaten to harm the business?

SWOT analysis involves using a matrix of the four elements, as shown in Figure 1.3.

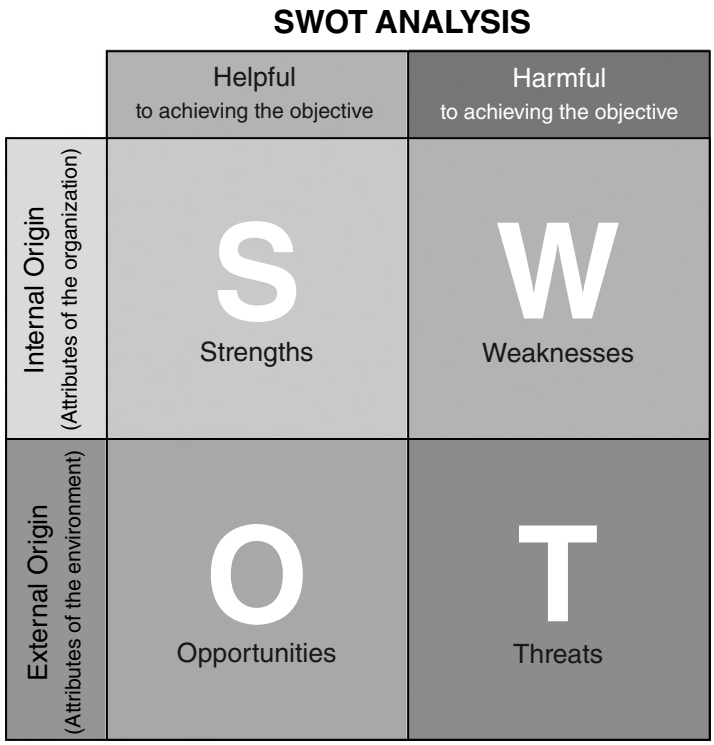
Capability Maturity Models

The Software Engineering Institute (SEI) at Carnegie Mellon University accomplished a great deal in developing the Capability Maturity Model Integration for Development (CMMi-DEV). *Capability maturity models* in other technology disciplines have also been developed, such as the Systems Security Engineering *Capability Maturity Model Integration (SSE-CMMI)* developed by the International Systems Security Engineering Association (ISSEA).

The CMMI uses five levels of maturity to describe the formality of a process:

- **Level 1: Initial** This represents a process that is ad hoc, inconsistent, unmeasured, and unrepeatable.

FIGURE 1.3 A SWOT matrix with its four components.



SOURCE: Courtesy of Xhienne.

- **Level 2: Repeatable** This represents a process that is performed consistently and yields the same outcome. It might not be well-documented.
- **Level 3: Defined** This represents a process that is well-defined and documented.
- **Level 4: Managed** This represents a quantitatively measured process with one or more metrics.
- **Level 5: Optimizing** This represents a measured process that is under continuous improvement.

Not all strategists are familiar with maturity models. Strategists unaccustomed to capability maturity models need to understand two important characteristics of the models and how they are used:

- **Level 5 is not the ultimate objective** Most organizations' average maturity level targets range from 2.5 to 3.5. There are few organizations whose mission justifies level 5 maturity. The cost of developing a level 5 process or control is often prohibitive and misaligned with the associated risks.

- **Each control or process can have its own maturity level** It is neither common nor prudent to assign a single maturity-level target to all controls and processes. Instead, organizations with skilled strategists can determine the appropriate level of maturity for each control and process. They need not all be the same. Instead, it is more appropriate to use a threat-based or risk-based model to determine an appropriate level of maturity for each control and process. Some will be 2, some will be 3, some will be 4, and a few might even be 5.

A common use of capability maturity models is to determine the current maturity of a process, along with analysis, to identify the desired maturity level, process-by-process and technology-by-technology.

Roadmap Development

Once strategic objectives, risk and threat assessments, and gap analyses have been completed, the strategist can begin to develop roadmaps to accomplish each objective. A roadmap is a list of steps required to achieve a strategic objective. The term *roadmap* is an appropriate metaphor because it represents a journey whose details might not always appear to contribute to the objective, though not necessarily in a straight line. But in a well-designed roadmap, each task and each project gets the organization closer to the objective.

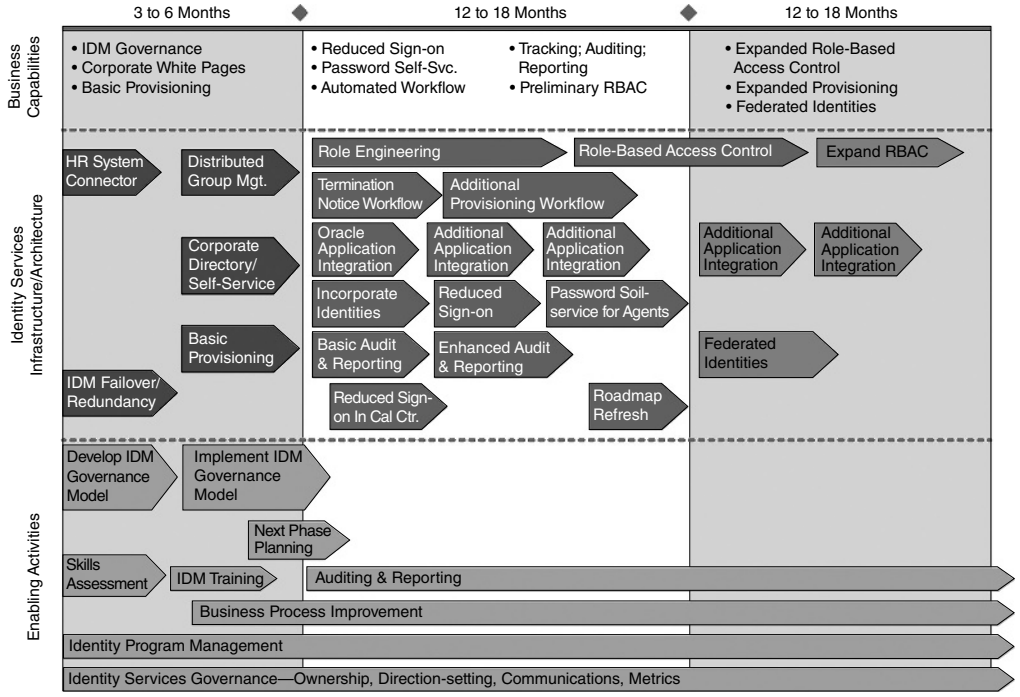
A roadmap is just a plan, but the term is often used to describe the steps an organization must take to achieve a long-term, complex, and strategic objective. Often, a roadmap is thought of as a series of projects—some running sequentially, others concurrently—that an organization uses to transform its processes and technology to achieve the objective.

Figure 1.4 depicts a roadmap for an 18-month identity and access management project.

A roadmap should be a top-down endeavor, following the usual hierarchy of control of an organization's operations. The roadmap can contain one or more of these:

- **Policy development** Sweeping changes in organizational practices around data protection and data management will likely require *policy* changes to codify expected behavior and system characteristics. While not generally required in most industries, it is common practice to structure the organization's security policy around one or more relevant standards or frameworks. Common standards and frameworks as a structure for security policy include NIST CSF, NIST SP 800-53, ISO/IEC 27001, HIPAA/HITECH, PCI DSS, and CIS CSC. Privacy controls can be adopted from ISO/IEC 27701 or the NIST Privacy Framework.
- **Controls development** The strategist might need to enact one or more controls within specific business processes to ensure desired outcomes related to data management and data protection. Generally, controls are developed (and retired) as a result of a risk assessment, and this might be the case when developing a privacy program strategy.

FIGURE 1.4 Sample roadmap for identity and access management initiative.



SOURCE: Courtesy of *Hi-Tech Security Solutions* magazine.

Exam Tip

CDPSE candidates are not expected to memorize the contents of control frameworks for the exam, but are expected to understand their purpose and use.

- **Standards development** Changes in policies, controls, or underlying technologies might necessitate the development or updating of one or more standards. While standards are often thought of in terms of topics like passwords and encryption, privacy-related standards can also be developed for topics like aggregation and de-identification.
- **Processes and procedures** Often, the purpose of a new privacy or security strategy is to increase the maturity of privacy- or security-related technologies and activities within an organization. Because many organizations' privacy and security maturity levels are low, important tasks are poorly documented or not documented at all. The desired increase in maturity might compel an organization to identify undocumented processes and procedures and assign staff to document them.

Exam Tip

The CDPSE exam requires that candidates understand the structure and use of policies, standards, guidelines, and procedures.

- **Roles and responsibilities** When the strategy involves changes in technologies or processes (as it usually does), this can, in turn, affect the roles and responsibilities of privacy and security personnel, IT workers, and perhaps other staff. When business processes are added or changed, this often requires adjustments to personnel roles and responsibilities. There might also be new positions that require developing charter documents and job descriptions.
- **Training and awareness** Execution of a new privacy or security strategy often has a broad reach, impacting technology as well as policies, standards, processes, and procedures. The results of these are new information, in many forms and for several audiences, including general privacy and security awareness, updated policies and procedures, and new information systems.

Developing a Business Case

Many organizations require a business case before approving significant expenditures for privacy or security initiatives. A *business case* is a written statement that describes the initiative and its business benefits. The following are the typical elements included in a business case:

- **Problem statement** This is a description of the business condition or situation that the initiative is designed to solve. The condition might be a matter of compliance, a finding in a risk assessment, or a capability required by a customer, partner, supplier, or regulator.
- **Current state** This is a description of the existing conditions related to the initiative.
- **Desired state** This is a description of the future state of the relevant systems, processes, or staff.
- **Success criteria** These are the defined items that the program will be measured against.
- **Requirements** This is a list of required characteristics and components of the solution that will remedy the current state and bring about the desired future state.
- **Approach** This is a description of the proposed steps that will result in the desired future state. This section might include alternative approaches that were considered, along with the reasons they were not selected. If the initiative requires the purchase of products or professional services, business cases can include vendor proposals. Alternatively, the business case might include a request for proposal (RFP) or request for information (RFI) that will be sent to selected vendors for additional information.

- **Plan** This will include costs, timelines, milestones, vendors, and staff associated with the initiative.

Mature organizations use an executive *steering committee* to evaluate business cases for proposed initiatives and make go/no-go decisions. Business cases are often presented to a steering committee as an interactive discussion, allowing business leaders to ask questions and propose alternative approaches.

Characteristics of business cases should include the following:

- **Alignment with organization** The business case should align with the organization's goals and objectives, risk appetite, and culture.
- **Alignment with regulations** A business case should cite and align with applicable privacy and data protection regulations.
- **Statements in business terms** Problem statements, current state, and future state descriptions should all be expressed in business terms.

Establishing Communications and Reporting

Effective communications and reporting are critical elements of successful privacy and security programs. Because success depends mainly on people, in the absence of effective communication, they won't have the information required to make good privacy- and security-related decisions. Without regard for privacy or information security, decision outcomes can lead to unacceptable risks and even harmful incidents.

These are common forms of communication and reporting that are related to privacy and information security:

- **Board of directors meetings** Discussions of strategies, objectives, risks, incidents, and industry developments keep board members informed about privacy and security in the organization and elsewhere.
- **Governance and steering committee meetings** Discussions of privacy and security strategies, objectives, assessments, risks, incidents, and developments guide decision-makers as they discuss strategies, objectives, projects, and operations.
- **Privacy and security awareness** Periodic communications to all personnel help keep them informed about changes in privacy and security policies and standards, good privacy and security practices, and risks they can encounter, such as phishing and social engineering attacks.
- **Privacy and security advisories** Communications on potential threats help keep affected personnel aware of developments that might require them to take steps to protect the organization from harm.
- **Privacy and security incidents** Communications internally as well as with external parties during an incident keep incident responders and other parties informed. Organizations typically develop privacy and security incident plans and playbooks in advance that include business rules for internal communications and for interactions with outside parties, including customers, regulators, and law enforcement.

- **Metrics** Key metrics are reported upward within an organization, keeping management, executives, and board members informed as to the effectiveness and progress of the organization's privacy and security programs.

When building or expanding a privacy or security program, it's best to use existing communication channels and add relevant privacy and security content to them, rather than creating new parallel channels. Effective privacy and security programs make the best use of existing processes, channels, and methods in an organization.

Obtaining Management Commitment

The execution of a privacy or security strategy requires management commitment. Without that commitment, the strategist will be unable to obtain funding and other resources to implement the strategy.

Getting management commitment is not always straightforward. Often, executives and board members are unaware of their fiduciary responsibilities and the potency of modern threats. Many organizations mistakenly believe they are unlikely targets for hackers and cybercriminals because they are small or uninteresting. Further, the common perception of executives and senior managers is that privacy and security tactical problems are solved with "firewalls and antivirus software," and that privacy and information security are in no way related to business issues and business strategy.

A privacy or security strategist in a situation where top management lacks a strategic understanding of privacy and security will need to inform top management (in *their* language) about one or more aspects of modern privacy or information security management. When success is elusive, it might be necessary to bring in outside experts to convince executives that their privacy or security manager is not trying to build a kingdom but is simply trying to build a basic program to keep the organization out of trouble. As part of developing an effective communication approach, the strategist should not use fear, uncertainty, or doubt to move the leadership team toward adopting the strategy. The better approach, as noted in this section, is to relate it to the leadership team in business terms and opportunities to improve business functions.

Strategy Constraints

While the development of a new strategy can bring hope and optimism to the privacy or security team, there is no guarantee that organizational changes can be implemented without friction or even opposition. Instead, the privacy and security manager should anticipate and be prepared to maneuver around, over, or through many constraints and obstacles.

No privacy or security manager plans to fail. However, failing to anticipate obstacles and constraints might result in the inability to execute even the best strategy. The presence of an excellent strategy, even with executive support, does not mean obstacles and constraints will simply step aside. Instead, obstacles and constraints reflect the realities of human behavior, as well as structural and operational constraints that might pose challenges for the privacy

and security manager and the organization as a whole. There is apt meaning to the phrase "the devil's in the details."

Typical constraints, obstacles, and other issues include:

- **Basic resistance to change** It is human nature to be suspicious of change, particularly when we as individuals have no control over it or say in it. Change is bad, or so we tend to think. "We've always done it this way," is a common refrain. Strategists need to consider methods for involving management and staff in anticipated changes, such as town hall meetings, surveys, and cross-functional committees.
- **Culture** Organizational culture can be thought of as the collective consciousness of all workers, regardless of rank. Privacy and security strategists should not expect to change the culture significantly; instead, they should work with the culture when developing and executing the privacy or security strategy.
- **Organizational structure** The strategist must understand the organization's command-and-control structure, often reflected in the organizational chart. However, there can be an undocumented aspect of the org chart that is more important: who is responsible for which activities, functions, and assets.
- **Staff capabilities** A strategy cannot be expected to succeed if the new or changed capabilities do not align with what staff members are able to do. A gap analysis to understand the present state of the organization's privacy or security program (discussed earlier in this chapter) needs to consider staff knowledge, skills, and capabilities. Where gaps are found, the strategy needs to include training or other activities to equip staff with the necessary skills and language. It is also important to understand who the true leaders and doers are in the organization so that the privacy leader can win their trust.

When an organization lacks staff with specific knowledge about privacy or security techniques or tools, it can look to external resources to augment its internal staff. The strategist needs to consider the costs and availability of these resources. Consultants and contracts in many skill areas are difficult to find; even larger firms can have backlogs of several months as a result.

- **Budget and cost** The strategist must determine, with a high degree of precision, all the hard and soft costs associated with each element of a strategy. Often, executive management will want to see alternative approaches; for example, if additional labor is required, the strategist might want to determine the costs of hiring additional personnel versus retaining consultants or contractors.
- **Time** Realistic project planning is needed so that everyone knows when project and strategy milestones will be completed. Project and strategy timelines must account for all business circumstances, including peak periods and holiday production freezes (when

IT systems are maintained in a more stable state), external events such as regulatory deadlines, audits, and other significant events that can impact schedules.

- **Legal and regulatory obligations** An organization might include items in its strategy that represent business capabilities required for legal or regulatory reasons. The enactment of new privacy laws might require considerable changes in practices in many organizations. The extraterritorial nature of some new privacy laws complicates this further.
- **Acceptable risk** Initiatives within the privacy or security strategy must align with executive management's risk appetite. However, increased pressure from privacy regulations might also be affecting risk appetite and forcing organizations to build more structure and defenses than they would otherwise.

The Obstacle of Organizational Inertia

Every organization has a finite capacity to undergo change. This is a fact that is often overlooked by overly ambitious strategists who want to accomplish a great deal in too short a time. I have coined the term *organizational inertia* to serve as an analogy to Newton's laws of motion: an object either remains at rest or continues to move at a constant velocity unless acted upon by a force. In an organization, this means that things will be done the same way until a force requires the organization to change what is done or how it is done. The greater the amount of change needed, the greater the outside force required to implement it.

The nature of organizational inertia, or its resistance to change, is threefold:

- Operational people changing their processes and procedures
- Learning curve
- Human resistance to change

Personal Information

Personal information is information about people, or as we like to say in the privacy business, *data subjects*. Because so many organizations use information technology to track, care for, service, or assist people, personal information often resides in information systems. As these systems became accessible from the Internet, cybercriminals realized they could *monetize* this information if they could obtain it.

Cybercriminals have been successfully stealing and monetizing personal information for at least 30 years, often through *identity theft*. The rate of identity theft rose dramatically in

the 1990s, prompting numerous laws and regulations to protect personal information. This has led to the growth of the privacy profession, including professional certifications like the CDPSE, the subject of this book.

Ask ten business and technology professionals for a definition of *personal information*, and you'll get ten different definitions. This reflects privacy laws, each of which has its own bespoke definition. If we wind back the clock a few years, we find early definitions, such as:

- **European Privacy Directive (1995)** "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."
- **California Senate Bill 1386** "'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."

Over many years, many U.S. states and numerous countries enacted privacy laws with their own definitions. Here are some more examples:

- **EU General Data Protection Regulation (GDPR)** "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (Note that this definition is identical to the 1995 European privacy directive.)
- **California Consumer Privacy Act (CCPA)** "'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers. (B) Any categories of personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories

or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99)." Note that the California Privacy Rights Act (CPRA) did not redefine "personal information," but retained and carried forward the existing definition from the CCPA. The CPRA added a new, narrower, higher-risk subcategory known as Sensitive Personal Information (SPI), which includes items such as Social Security numbers, driver's license numbers, passport numbers, and account login credentials.

- **Health Insurance Portability and Accountability Act (HIPAA)** "*Protected health information* means individually identifiable health information … that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium."

These and many other laws have settled into a more-or-less consistent theme for what privacy professionals call *personally identifiable information (PII)*, which generally includes:

- Name
- Date of birth
- Contact information (any of: telephone number, email address, residence address, IP address, and so forth)
- Contextual information (any of: bank account number, Social Security number, medical record number, driver's license number, and so forth)
- Additional information (any of: religious preferences, sexual preferences, political preferences/membership)

For most organizations and government agencies, information about the following classes of people is generally included:

- Employees
- Customers
- Donors
- Constituents
- … and possibly others

If, upon reading this, you are a bit confused, don't worry: this is the privacy profession today. We are responsible for protecting information about people from misuse, abuse, and theft. With multiple laws, regulations, and standards that partly overlap, we are accountable

for developing policies, processes, and safeguards to protect information about persons, including employees, customers, and others.

PII: Build Your Own Definition

Every organization is different from every other in terms of industry, business model, physical location, the locations of employees and customers, and the laws and regulations it is required to comply with. As such, many organizations develop a bespoke definition of PII that accounts for all these factors.

Some organizations take a somewhat different approach, separating employees from customers, each with their own PII definitions.

Privacy Principles

Privacy principles provide the conceptual foundation for how personal data is collected, used, and protected across systems and organizations. They translate legal obligations and ethical expectations into consistent, actionable guidance applicable throughout the data lifecycle. Frameworks such as the OECD principles and emerging models like FAIR (Factor Analysis of Information Risk, discussed in Chapter 3) help structure thinking about accountability, risk, and value. Core concepts, including transparency, consent, purpose limitation, and privacy by design, establish expectations for responsible data handling. Together, these principles enable organizations and privacy professionals to align governance, engineering, and operations, ensuring that privacy is not treated as an afterthought but as an integral design requirement.

Privacy by Design

Privacy and security by design is a concept that reinforces the need to have privacy and security considerations incorporated into systems and applications by default. In other words, the product is designed with privacy and security as priorities, along with any other functional purposes it serves.

Exam Tip

Implementing security and privacy by design involves not only development processes but a change in organizational culture.

Privacy by design is based on seven foundational principles:

- **Proactive not reactive; preventive not remedial** The privacy-by-design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. Privacy by design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred; it aims to prevent them.
- **Privacy embedded into design** Privacy by design is embedded in the design and architecture of IT systems as well as business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system without diminishing its functionality.
- **Privacy as the default setting** Privacy by default seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing to protect their privacy, it should remain intact. No action should be required of the individual to protect their privacy.
- **Full functionality—positive-sum, not zero-sum** Privacy by design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by design avoids the pretense of false dichotomies, such as privacy versus security, demonstrating that it is possible to have both.
- **End-to-end security—full lifecycle protection** Privacy by design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved—strong security measures are essential to privacy, from start to finish. This ensures that all data is securely retained and then securely destroyed at the end of the process, in a timely fashion. Thus, privacy by design ensures end-to-end, cradle-to-grave secure lifecycle management of information.
- **Visibility and transparency—keep it open** Privacy by design seeks to assure all stakeholders that whatever the business practice or technology involved, it is, in fact, operating according to the stated promises and objectives, subject to independent verification. Its parts and operations remain visible and transparent to users and providers alike.
- **Respect for user privacy—keep it user-centric** Privacy by design requires architects and administrators to keep the interests of the individual uppermost by offering measures such as strong privacy defaults, appropriate notice, and user-friendly empowerment options.

Business application architectures, designs, data flows, and configurations all must contribute to and support privacy and security. The *systems development lifecycle* represents the business processes used to develop, maintain, and operate business applications. It must

include steps to ensure that new and existing information systems do not impact security and privacy in unexpected ways. Policies and standards must also support security and privacy principles to ensure that personal information is adequately protected and properly used. Ongoing operations must likewise ensure that the security and privacy of systems are not compromised and that continuous monitoring is employed to detect security and privacy incidents early so that they might be contained.

Consent

In the context of data privacy, *consent* is a distinct action taken by a data subject to grant an organization permission to collect and/or process their personal information. Consent must be given freely, in a specific context, be revocable, and comply with applicable laws.

There are several ways in which consent is given and obtained, including the following:

- **At the time of data collection** When a data subject provides one or more items of personal information to an organization, the data subject also provides consent for the collection and processing of that information. In an online context, consent often takes the form of a checkbox with words citing agreement with a privacy policy that can be read in its entirety. On a paper form, consent often appears in the signature block.
- **Prior to data collection** When a data subject is establishing a relationship with an organization, a part of the agreement can include obtaining consent for future data collection.
- **Consent obtained through a third party** In some instances, it is not feasible for an organization to collect consent directly from a data subject. For example, in the case of advertising specifically chosen for and delivered to a data subject, the organization displaying the advertising will have collected consent "for other uses," including advertising. The advertiser will have been assured that consent has been obtained from all data subjects to whom the advertiser is displaying ad content.

Regardless of the method used to obtain consent, organizations must record the specific date, time, stipulations, and circumstances under which that consent was obtained. Organizations need to be quite specific regarding this collection. For instance, if an organization collects personal information for a specific context or event, and consent to use that information is limited to that context or event, the organization cannot later use that information for other contexts or events.

GDPR and CCPA/CPRA treat consent differently. Under the GDPR, consent is only one of several lawful bases for processing personal data. It is required only when no other lawful basis (such as contract, legal obligation, or legitimate interests) applies. When used, consent must be freely given, specific, informed, and unambiguous, and, in certain cases, explicit (e.g., for special categories of data).

In contrast, CCPA/CPRA does not rely on consent as the primary basis for processing. Instead, it generally permits the collection and use of personal information with required notice. It grants consumers the right to opt out of specific activities, particularly the sale or sharing of personal information, and to limit the use of sensitive personal information.

Transparency

In the context of privacy, *transparency* refers to the extent to which an organization discloses its practices regarding the collection, protection, and use of personal information. Transparency often begins with an organization publishing an external privacy policy, often called a *notice of privacy practices (NOPP)*, in which it fully discloses the collection, protection, use, distribution, and disposal of personal information. The NOPP will likely also contain guidance for data subjects who want to make inquiries, lodge complaints, and request corrections or the removal of their information.

Transparency requires trust. In terms of a posted privacy policy or NOPP, organizations need to "say what they do, and do what they say." Trust is hard to earn and easy to lose, so organizations must take transparency seriously. Privacy laws, described later in this chapter, require transparency and hold organizations accountable for their information collection and handling practices.

Minimization

In privacy, the concept of *minimization* stresses that the collection of personal information should include *only* the records and data fields that are required, and no more. These concepts include:

- **Collect only the personal information required for processing** Any personal items not used should not be collected. For instance, if an organization does not require a subject's date of birth to perform processing, then the date of birth should not be collected.
- **Retain personal information only as long as required** When an organization no longer needs personal information about a data subject, it should be discarded.

The reason for data minimization is this: data that is collected and needed provides value to the organization, but also poses a liability in the case of theft. However, data that is collected but *not* needed represents only liability for the organization, particularly if it is stolen.

Purpose Limitation

In privacy, the concept of *purpose limitation* states that personal information should be used only for explicitly stated purposes described in the NOPP. Any organization that collects personal information for one purpose must not subsequently use it for other purposes unless it obtains consent for the new purpose.

Legal Basis

In the context of data privacy and privacy regulations, organizations must identify the specific *legal basis* for collecting and/or processing personal information. Simply put, it must be lawful for the organization to collect and use data subjects' personal information, and the organization must be able to cite specifically how it is lawful.

In Article 6.1, the GDPR provides five possible avenues of legal basis (quoting directly from GDPR):

- *The data subject has given consent to the processing of their personal data for one or more specific purposes*;
- *Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*;
- *Processing is necessary for compliance with a legal obligation to which the controller is subject*;
- *Processing is necessary in order to protect the vital interests of the data subject or of another natural person*;
- *Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*;
- *Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection. [This does not apply to public authorities in the performance of their duties.]*

EU member states might include additional provisions.

The CCPA/CPRA do not treat this in the same way as the GDPR. Instead, entities subject to the CCPA/CPRA must generally comply with the law. Certain use cases, such as healthcare and employment, with specific provisions, are cited.

Legitimate Interest

The term *legitimate interest* is defined in the GDPR as one of six bases for the lawful collection and processing of personal information. One might consider legitimate interest a loophole, but the author's opinion is that this provision was included so that the GDPR did not need to enumerate every possible use of personal information (which would soon be out of date, requiring frequent updates to the law).

Legitimate interest provides organizations with a basis for collecting and processing personal information when they benefit from doing so. But it doesn't end there: the real issue of legitimate interest is that organizations must balance their interests with those of the data subject.

Online advertising is an interesting case to consider. Advertisers have an interest in serving advertising content to readers and viewers. To stay in business and earn advertising revenue (which is the business model for a considerable number of websites), advertisers claim that readers and viewers benefit (their interest) in advertising that is aligned with topics of interest to them (the readers' and viewers' interest). Thus, there is an argument that online advertising benefits both the advertiser (and the website operator) and the viewer (the data subject).

Organizations are cautioned against relying on legitimate interest too readily. Some long-established industry and business practices might be forever altered because of GDPR, CCPA, CPRA, and other privacy laws.

ISACA Privacy Principles

ISACA has published a privacy-principles guide that includes the following topics:

- Management
- Notice
- Choice and consent
- Collection
- Use, retention, and disposal
- Access
- Disclosure to third parties
- Security
- Quality
- Monitoring and enforcement

ISACA's *Privacy Principles and Program Management Guide* is available from https://store.isaca.org.

Privacy Engineering Principles

Engineering is the disciplined application of scientific and mathematical principles to design, build, and operate systems that reliably meet defined objectives within real-world constraints. It begins with a clear problem definition and requirements, followed by a systematic decomposition of complex systems into manageable components. Engineers apply modeling, analysis, and empirical testing to evaluate alternatives, optimize performance,

and manage trade-offs among cost, quality, safety, and time. Design decisions are guided by repeatability, scalability, and maintainability, ensuring that solutions perform consistently under expected conditions and degrade gracefully under stress. Risk management is integral, incorporating safety margins, failure analysis, and controls to reduce uncertainty and unintended consequences. Finally, engineering is inherently iterative: solutions are refined through continuous feedback, measurement, and improvement, grounded in evidence rather than assumption.

Privacy engineering is the application of these engineering principles with the twin objectives of privacy: identifying and protecting personal information, and ensuring that personal information is used only as directed by policy and approved by management.

Now, let us go into greater detail and speak to individual principles of privacy engineering, some of which were implied earlier in this discussion. NIST, in its publication NISTIR 8062, *Introduction to Privacy Engineering and Risk Management in Federal Systems*, describes privacy engineering principles as follows:

- **Predictability** Enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system. The purpose of predictability is to establish trust and accountability through transparency.
- **Manageability** Providing the capability for granular administration of PII, including alteration, deletion, and selective disclosure.
- **Disassociability** Enabling the processing of PII or events without association with individuals or devices beyond the operational requirements of the system. This principle calls for data minimization: collecting *only* what personal information is truly needed, de-identifying when possible, and retaining it for the shortest possible time.

Privacy engineering is managed through *privacy governance*, including policies, roles and responsibilities, and processes such as the *systems development lifecycle (SDLC)*, in which key privacy-by-design activities are required and reviewed.

Privacy is wholly dependent upon sound data governance and data management, which are discussed in Chapters 5 and 6.

Privacy Laws, Regulations, and Standards

Laws passed by governments at the national, state, and provincial levels impose requirements on organizations that store or process personal information about natural persons. These laws have been enacted in response to citizens' outcry over the abuse of their personal information and violations of their right to privacy as technology and the Internet

have become part of our daily lives. Activities such as telemarketing and tracking people's locations and habits have been the focus of growing concerns by citizens and privacy advocates. Advances in the capabilities of information systems and data mining of large databases containing personal information have enabled practices that many private citizens find inappropriate and even intrusive. Abuses of such capabilities would allow the creation of a new, highly invasive form of a surveillance police state, which is not difficult to imagine, as some governments around the world are already there. Legislators in many countries have sought to counterbalance these capabilities by defining the rights of natural persons concerning the data that is collected about them and used in various ways.

The most influential privacy laws include the EU GDPR, the U.S. Health Insurance Portability and Accountability Act (HIPAA), the U.S. Fair Credit Reporting Act (FCRA), the U.S. Electronic Communications Privacy Act (ECPA), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the CCPA, and the China Cybersecurity Law (CCSL). These and other laws are discussed in the remainder of this section. This is not intended to be an exhaustive or authoritative list, but instead a sampling of better-known privacy laws.

Privacy protection regulations fall into four categories:

- **Comprehensive** A single unified legal framework governing personal information across all sectors. Examples: GDPR, CCPA/CPRA.
- **Sectoral** Laws that are applied to specific industry sectors. Examples: HIPAA, GLBA.
- **Self-regulatory** Organizations define their own policies and practices, following industry standards. Examples: OECD privacy principles and Fair Information Practice Principles (FIPPs).
- **Co-regulatory** Government-industry partnerships in which laws set high-level requirements and industries develop detailed rules.

Because privacy and data amendment protection laws are being rapidly enacted and changed, organizations and privacy professionals must devise a way to remain fully aware of new and evolving laws.

EU General Data Protection Regulation

One of the most notable modern privacy laws, the *General Data Protection Regulation (GDPR)* enacts sweeping requirements upon organizations within and beyond the European Union that store, process, or transmit personal data about EU citizens and residents. The GDPR was passed in April 2016 and became effective in May 2018. The main privileges enacted by the GDPR include the following:

- **Rights of data subjects** Any organization collecting information about EU residents is required to operate transparently when collecting and using their personal information.

Chapter III of the GDPR defines eight data subject rights that have become foundational for other privacy regulations around the world:

- *Right to access personal data* Data subjects can access the data collected on them.
- *Right to rectification* Data subjects can request modifications to their data to correct errors and update incomplete information.
- *Right to erasure* Also referred to as *the right to be forgotten*, this right allows data subjects to request that their personal data be erased from an entity's processing activities.
- *Right to restrict processing* In certain circumstances, data subjects can request that processing of their personal data be stopped.
- *Right to be informed* Data subjects must be notified of what information is being collected at or before collection, and of its use.
- *Right to data portability* Data subjects can request that their personal data be provided in a commonly used, machine-readable format.
- *Right to object* Data subjects can object to the processing of their data when a controller attempts to argue that legitimate grounds for processing override the data subject's interests, rights, and freedoms, or that processing is for legal purposes.
- *Right to reject automated individual decision-making* Data subjects can refuse the automated processing of their personal data for decision-making.

- **Definitions of data controller and data processor** The GDPR defines a *data controller* as an organization that directs the use of personal data. A *data processor* is an organization that processes personal data as directed by a data controller. Controllers and processors are required to maintain records regarding the collection and processing of personal information.
- **Data protection and privacy by design and by default** Organizations are required to design, operate, and maintain their business processes and information systems with privacy and security as part of their default design.
- **Cybersecurity** Organizations that process personal information are required to implement cybersecurity measures to protect that data.
- **Breach notification** Organizations are required to notify supervisory authorities and affected data subjects in the event of a privacy or security breach of personal data.
- ***Data protection impact assessment (DPIA)*** The DPIA is a formal process to identify and minimize the data protection risks of a data processing activity. Organizations are required to perform DPIAs whenever they implement new systems or make significant changes to business processes or information systems.
- ***Data protection officer (DPO)*** Organizations are required to appoint a DPO if they process personal data on a large scale. The DPO is expected to have expert knowledge of data protection law and practices.

- **Certification** The GDPR permits the creation of certification authorities and the voluntary certification of organizations that process personal data.
- ***Cross-border data transfers*** The GDPR contains rules regarding the transfer of personal data out of the European Union.
- ***Binding corporate rules*** The GDPR accommodates the use of binding corporate rules that multinational organizations might enact to ensure the protection and appropriate use of personal data when transferred outside the European Union to their overseas systems.
- ***Supervisory authority*** Each member state in the EU establishes a supervisory authority responsible for monitoring GDPR compliance.
- **Penalties** The GDPR authorizes supervisory authorities to impose fines on organizations that violate its terms. Administrative fines can be as high as €20 million or 4% of global turnover, whichever is greater.

The GDPR claims to have *extraterritorial* jurisdiction over companies not based in the European Union that provide goods or services to EU citizens in EU member states. This claim of jurisdiction beyond its own borders has been seriously tested in courts, with numerous enforcement actions and cross-border rulings established. However, the enforcement of extraterritoriality has split into two types of situations. For U.S.-based organizations with operations in the EU, data protection authorities fined Marriott £99 million for a 2018 breach and Google €50 million for alleged abuses of privacy settings. For U.S.-based organizations with no EU establishment or assets, GDPR fines have been unenforceable. Subsequent fines and appeals against non-EU companies can result in additional types of cases.

U.S. Health Insurance Portability and Accountability Act

Enacted in 1996, the *Health Insurance Portability and Accountability Act (HIPAA)* includes two rules that address the protection of *protected health information (PHI)* and *electronic protected health information (ePHI)*. *Covered entities* are organizations that store or process medical information and are subject to one or both of these rules:

- **Security rule** This part of HIPAA requires that organizations implement several administrative, physical, and technical safeguards to protect ePHI. Many of these controls are compulsory, while others are "addressable" (an organization can rationalize their disuse).
- **Privacy rule** Effective in 2003, this part of HIPAA requires that organizations protect PHI, whether in electronic or hardcopy form.

Additional provisions of HIPAA are not related to security or privacy.

HIPAA defines various civil and criminal penalties for organizations that violate the law. Covered entities are required to enter into *business associate agreements (BAAs)* with all third parties that store or process ePHI on their behalf.

Health Information Technology for Economic and Clinical Health Act

Enacted in 2009, the *Health Information Technology for Economic and Clinical Health (HITECH)* law extends the Security Rule and Privacy Rule in HIPAA by expanding security breach notification requirements and expanding the disclosures of the use of a patient's PHI.

U.S. Fair Credit Reporting Act

Enacted in 1970, the *Fair Credit Reporting Act (FCRA)* provides visibility, remedies, and assurances, including civil liability, that the information in consumers' credit histories is accurate. Since credit reports are used by banks and other financial institutions (as well as employers in many states for making hire/no-hire decisions), the FCRA provides consumers with a means to obtain copies of their credit reports and procedures for correcting erroneous information in those reports.

FCRA is an early example of a privacy law that provides individuals with the ability to know what personal information is being stored, how it is used, and how to obtain copies and request corrections.

If consumers' rights are violated, they can recover damages, attorney fees, and court costs, and punitive damages can be awarded if actions against them were willful.

California Consumer Protection Act & California Privacy Rights Act

Effective January 1, 2020, the *California Consumer Privacy Act (CCPA)* is a state law designed to enhance California residents' privacy rights. Provisions of the CCPA give California residents certain rights, including the following:

- Knowledge of what personal information is being collected
- Notification of whether such personal information is subsequently transferred or disclosed to another party
- The ability to prohibit an organization from transferring or selling its personal information
- The ability to examine the personal information held by organizations, with the right to request that the information be corrected or removed
- The freedom from discrimination should they choose to exercise their privacy rights

Californians can sue for damages when nonencrypted and nonredacted personal information is subject to unauthorized access, exfiltration, theft, or disclosure due to a business's failure to implement and maintain reasonable security procedures.

Like the EU GDPR, the CCPA claims jurisdiction over companies not located in California if they collect personal information about California residents. And like the GDPR, this provision has yet to be tested in court.

Made effective on January 1, 2023, the *California Privacy Rights Act (CPRA)* extends the CCPA by:

- Introducing a new information category known as *Sensitive Personal Information (SPI)*
- Expanding consumer rights, including the right of information correction, limitations on sensitive data use, and rights to know how data is collected, shared, and retained
- Introducing data minimization, purpose limitation, and retention principles
- Expanding liability for contractors and service providers
- Increasing protection for minors
- Expanding risk and governance requirements
- Establishing the California Privacy Protection Agency that can issue regulations, investigate violations, and enforce the law

Further expansion of the CPRA, adopted by the California Privacy Protection Agency (CPPA) in June 2025 and effective in January 2026, includes enhancements concerning *automatic decision-making technology (ADMT)*, risk assessments, cybersecurity audits, and the lookback period for consumer data access requests.

Canadian Personal Information Protection and Electronic Documents Act

The *Personal Information Protection and Electronic Documents Act (PIPEDA)* took effect in 2000 and aims to protect consumer data privacy in the context of e-commerce. In part, PIPEDA was enacted to provide assurances to European countries and consumers that their personal information present in Canadian companies' information systems would be safe and free from abuse.

PIPEDA also gives Canadians the right to know why organizations collect, use, or disclose their personal information, and to be assured that their information will not be used for any other purpose. They can further know who within the organization is responsible for protecting their information. They can contact the organizations to ensure that their personal data is accurate and can lodge complaints if they believe their privacy rights have been violated. Canadian companies must obtain consent to collect personal information, and they cannot refuse to provide service to a Canadian citizen if the citizen refuses to provide such consent.

China's Cybersecurity and Personal Information Protection Laws

Enacted in 2016 and effective in 2017, the *China Cybersecurity Law (CSL)* consists of three main parts:

- **Data protection** Organizations holding personal information about Chinese citizens must take measures to protect that information.
- **Data localization** Organizations collecting information about Chinese citizens must keep such data within China. Organizations that want to transfer data out of China must undergo a data assessment by the Chinese government.
- **Cybersecurity** Organizations are required to implement controls to prevent malware, intrusions, and other attacks. The law includes mandatory standards, assessments, and certifications for network devices.

CSL's data protection principles resemble those of the GDPR. Both laws require that organizations inform citizens if they hold their personal data, explain how their personal data is used, identify collection methods, and obtain consent for continued use.

CSL was amended in 2025, effective January 1, 2026, to strengthen enforcement penalties and align it with other data governance laws.

In 2021, China enacted the *Personal Information Protection Law (PIPL)* that governs how organizations collect, process, and transfer personal information.

Brazilian General Data Protection Law (LGPD)

Enacted in 2019 and effective in August 2020, the LGPD is similar to the EU GDPR. The LGPD establishes a National Data Protection Authority, designated as the federal agency responsible for overseeing data protection regulation.

The LGPD establishes some individual rights over personal data, many of which are similar to those provided by the GDPR. However, the LGPD also provides additional rights, including access to information about entities with which an organization has shared the individual's personal data.

Like the GDPR and the CCPA, the LGPD claims jurisdiction over companies not located in Brazil if one of the following criteria is met:

- The processing operation is carried out in Brazil
- The purpose of the processing activity is to offer or provide goods or services to individuals located in Brazil
- The personal data was collected in Brazil

Privacy Laws Enforced by the FTC

In the United States, the Federal Trade Commission (FTC), the agency that monitors the rights of consumers, has brought legal action against scores of companies in alleged violation of consumer protection laws, including violations of posted privacy policies, breaches of personal information, improper collection of personal data without consent, and failures to protect personal information.

The FTC enforces more than 70 laws, including these:

- Federal Trade Commission Act, which protects consumers from unfair and deceptive practices
- Children's Online Privacy Protection Act (COPPA), which protects children's online privacy, particularly those under age 13
- Do-Not-Call Implementation Act, which provides for consumers to opt out of all telemarketing calls
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), which prevents misleading advertising and requires consumers to opt out
- Gramm-Leach-Bliley Act (GLBA), which protects and secures the privacy of consumer personal information by financial institutions
- HITECH, which extends the scope of HIPAA
- Identity Theft Assumption and Deterrence Act, which provides a central clearinghouse for identity theft complaints
- Fair Credit Reporting Act, which protects personal information collected by consumer credit bureaus, medical information companies, and tenant screening services
- The Clayton Act, which prevents illegal contracts, mergers, and acquisitions

Other Legal Obligations

In addition to abiding by applicable laws and regulations, organizations can negotiate additional terms and conditions regarding the protection of personal information. Such obligations might be related to specific services rendered by third-party service providers that store or process personal information on behalf of other organizations. For instance, a service provider might comply with all applicable laws, agree to specific protective measures, undergo periodic audits or examinations, or provide specific reporting regarding the storage or use of personal data.

Privacy Documentation and Records

Documentation is an inclusive term that describes many types of written artifacts, including but not limited to policies, standards, charters, processes, procedures, requirements, and others. Organizations that strive to operate with intentionality and consistency must document their principles and practices and make them available to personnel so they can conform to them.

Records are the written descriptions of business events such as meeting minutes, contracts, financial transactions, decisions, purchase orders, event logs, and reports.

Privacy programs are found to have many types of documentation and records, including these:

- **Policies** Statements defining required behavior and characteristics of processes and systems. A policy generally describes *what* must be (or not be) done. All personnel in an organization are required to comply with policy.
  - *Internal policies* An internal privacy policy, directed at an organization's workforce, defines required and prohibited behaviors regarding the collection, handling, distribution, and disposal of personal information. These internal policies must be consistent with public-facing policies.
  - *External policies, aka notice of privacy practices (NOPP)* External-facing policies, often published on an organizational website, that describe the collection, use, distribution, and disposal of personal information, as well as guidelines for making inquiries and lodging complaints.
- **Standards** Statements that describe *how* (or *with what*) policies are to be carried out. All personnel in an organization are required to comply with standards. Some of the types of standards that an organization might have include:
  - *Methodology standards* Statements that specify methodologies to be used, such as systems development lifecycle methodologies like Agile.
  - *Technology standards* Statements that specify technologies to use, such as encryption algorithms.
  - *Protocol standards* Statements that specify protocols to use, such as network routing protocols or network encryption protocols.
  - *Vendor standards* Statements that specify which vendors are used for various products and services. For instance, an organization might establish Cisco Systems as a networking equipment vendor.
- **Guidelines** Optional guidance on how policies and standards can be carried out.
- ***Program charter*** A formal document describing a privacy (or any other) program, including mission and objectives, roles and responsibilities, principal processes and procedures, *program management*, and the location of documentation and records.
- **Risk register** A living business record containing all risks identified to date, along with detailed information about each.
- **Event logs** Usually found in information systems, event logs contain the individual events, such as login attempts, permission changes, changes to data, and configuration changes.
- ***Corrective action plan*** A plan of action that describes steps to be taken to correct a defect or anomaly.
- ***Preventive action plan*** A plan of action that describes steps to be taken to prevent an incident, defect, or anomaly.

- ***Contracts*** Binding legal agreements between organizations that are enforceable in a court of law.
- **Meeting minutes** A written record of the proceedings of official meetings.
- **Decision log** A written record of key decisions made, such as risk treatment decisions (these are also to be included in a risk register).
- **Issues log** A written record of program-level issues that must be dealt with at some point.

The annual review of documents is a recommended practice to ensure that policies, standards, procedures, and related materials are current. Auditors often consider any document not reviewed in over a year as ineffective.

Regulations and standards often include explicit and implicit requirements for the existence of documentation and records.

Summary

Privacy governance is the set of established governance activities that provide management with visibility and control over an organization's privacy program and operations. Governance begins with the development of strategic objectives that are translated into action plans, roles and responsibilities, policies, procedures, standards, and guidelines.

Privacy governance cannot succeed in the absence of data, security, and IT governance, all of which should be considered prerequisites. Factors influencing privacy governance include the nature of personal information, applicable laws, risk appetite, and societal expectations.

Activities required to protect personal information include risk management, process management, event management, incident response, metrics and reporting, resource management, and monitoring.

A privacy program must be business-aligned; that is, it supports the organization's mission, goals, objectives, culture, and practices. Further, a privacy program must operate within an organization's risk appetite, tolerance, and capacity.

A strategy is a plan to achieve an objective. Organizations building or improving their privacy programs develop a strategy to implement new and improved policies, practices, processes, records, tools, and more. To develop a strategy, it's necessary to define the desired future state of a privacy program, understand its current state, and perform a gap analysis to detail the improvements needed. Resources that describe the current state include risk assessments, threat assessments, vulnerability assessments, maturity assessments, risk register,

audits, policies, standards, processes, architecture, controls, staff skills and knowledge, metrics and reports, business impact analysis, and culture.

A strengths, weaknesses, opportunities, and threats (SWOT) diagram can help a strategist visually understand a current privacy program. A maturity model can help a strategist better understand the maturity level of various components of privacy operations.

Armed with the foregoing, a strategist will develop a roadmap, which is a detailed plan of action to achieve the desired future state of the privacy program. Often, the privacy leader will need to develop a business case to sell the plan to executive management, who will need to provide resources for the strategy to be implemented.

Privacy leaders must recognize expected pockets of resistance to a strategic plan, including basic human resistance to change, as well as culture, organizational structure, staff capabilities, budget, time, and organizational priorities. Privacy is rarely a top priority in any organization.

Personal information is information about people, often including considerable detail, such as non-public information, such as addresses, phone numbers, health, financial, political, religious, sexual, and other details. There is no single universal definition of personal information, although definitions in various laws, regulations, and standards share recurring elements.

Several privacy operational practices have been developed over the years and are described in various standards. These practices include privacy by design, consent, transparency, legal basis, and legitimate interest. Privacy principles have been developed and published by ISACA, OECD, FAIR, and others.

As defined by NIST, privacy engineering principles are predictability, manageability, and disassociability. Privacy engineering is managed through privacy governance, including policies, roles and responsibilities, and processes such as the systems development lifecycle.

Numerous privacy laws and regulations exist today, including the European General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the U.S. Fair Credit Reporting Act, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the China Cyber Security and Personal Information Protection Laws, the Brazil General Data Protection Law (LGPD), and many others.

Privacy programs will have numerous documents and records, including policies, standards, guidelines, processes, procedures, a program charter, a risk register, event logs, corrective and preventive action plans, contracts, meeting minutes, a decision log, and an issues log.

Exam Essentials

Understand the purpose of privacy governance. Privacy governance provides structure, oversight, and accountability for how personal information is collected, used, protected, and managed. It ensures alignment with business objectives, regulatory requirements, and stakeholder expectations.

Know the components of a privacy program. A privacy program includes policies, standards, procedures, controls, metrics, and reporting mechanisms that collectively govern the collection, handling, and protection of personal information. These components must be applied consistently and reviewed regularly.

Understand the definition and scope of personal information. Personal information refers to data that identifies or can be linked to an individual, directly or indirectly. Definitions vary across laws, but generally include identifiers, sensitive attributes, and contextual data.

Understand the key privacy principles. Core principles such as privacy by design, transparency, consent, purpose limitation, and data minimization guide responsible data handling. These principles translate legal and ethical expectations into operational practices.

Understand lawful bases for processing personal data. Under regulations such as GDPR, processing must be justified by a lawful basis (e.g., consent, contract, legal obligation, legitimate interests). Consent is only one option and must meet strict requirements when used.

Recognize the role of governance structures and accountability. Effective privacy governance includes clearly defined roles such as data owners, privacy officers, and oversight bodies. Models such as the three lines of defense help ensure accountability and independent assurance.

Understand the role of privacy documentation and records. Documentation such as policies, notices, risk registers, and decision logs provides evidence of compliance and supports consistent operations. Records must be maintained, current, and aligned with regulatory expectations.

Review Questions

1. What is the primary purpose of privacy governance in an organization?
   - **A.** To implement security controls for IT systems
   - **B.** To ensure alignment of privacy practices with business objectives and legal requirements
   - **C.** To eliminate all privacy risks
   - **D.** To centralize all data processing activities
2. Which of the following best describes personal information?
   - **A.** Any data stored in a database
   - **B.** Data that is encrypted
   - **C.** Information that identifies or can be linked to an individual
   - **D.** Only financial and medical records
3. Under GDPR, which of the following is NOT a lawful basis for processing personal data?
   - **A.** Consent
   - **B.** Contractual necessity
   - **C.** Legitimate interests
   - **D.** Business convenience
4. Which privacy principle requires that personal data be collected only for specific, defined purposes?
   - **A.** Transparency
   - **B.** Purpose limitation
   - **C.** Data minimization
   - **D.** Accountability
5. What is the primary responsibility of the first line of defense in privacy governance?
   - **A.** Conduct independent audits
   - **B.** Define policies and standards
   - **C.** Implement and operate privacy controls
   - **D.** Report to regulators
6. Which of the following is a key characteristic of valid consent under GDPR?
   - **A.** Implied through inactivity
   - **B.** Freely given and specific
   - **C.** Permanent and irrevocable
   - **D.** Required for all processing activities

7. What is the primary role of the second line of defense?
   - **A.** Execute business processes
   - **B.** Provide independent assurance
   - **C.** Establish policies and monitor compliance
   - **D.** Perform system administration

8. Which document describes how an organization collects, uses, and shares personal information externally?
   - **A.** Internal audit report
   - **B.** Risk register
   - **C.** Privacy notice
   - **D.** Incident log

9. What is the main objective of privacy by design?
   - **A.** Add privacy controls after deployment
   - **B.** Minimize system costs
   - **C.** Embed privacy into system from the start
   - **D.** Eliminate the need for consent

10. Which of the following best describes data minimization?
    - **A.** Encrypt all data
    - **B.** Retain data indefinitely
    - **C.** Collect only the data necessary for a specific purpose
    - **D.** Share data across departments

11. What is the purpose of a risk register in a privacy program?
    - **A.** Store personal data
    - **B.** Track identified risks and treatment decisions
    - **C.** Log system events
    - **D.** Record employee training

12. Which of the following is the best example of transparency?
    - **A.** Encrypting data
    - **B.** Publishing a clear privacy notice
    - **C.** Conducting internal audits
    - **D.** Limiting data access

13. What is the primary function of internal audit in privacy governance?
    - **A.** Implement controls
    - **B.** Monitor daily operations
    - **C.** Provide independent assurance
    - **D.** Define policies

14. Which of the following best describes "legal basis" under GDPR?
    - **A.** A justification for collecting personal data
    - **B.** A contractual agreement with vendors
    - **C.** A privacy policy requirement
    - **D.** A security control framework

15. What is the primary purpose of a Data Protection Impact Assessment (DPIA)?
    - **A.** Monitor employee performance
    - **B.** Identify and mitigate privacy risks in processing activities
    - **C.** Audit financial systems
    - **D.** Classify data assets

16. Which of the following best describes accountability in privacy governance?
    - **A.** Delegating all responsibility to IT
    - **B.** Documenting and demonstrating compliance with privacy requirements
    - **C.** Eliminating all risks
    - **D.** Avoiding regulatory oversight

17. Which privacy law introduced the concept of Sensitive Personal Information (SPI) in California?
    - **A.** HIPAA
    - **B.** GDPR
    - **C.** CPRA
    - **D.** FCRA

18. What is the primary purpose of privacy documentation?
    - **A.** Replace operational controls
    - **B.** Provide evidence and guidance for consistent practices
    - **C.** Eliminate audits
    - **D.** Reduce system complexity

19. Which of the following best describes the difference between data and information?
    - **A.** Data is always structured; information is not
    - **B.** Data is raw; information is data with context and meaning
    - **C.** Information is always digital
    - **D.** There is no difference
20. Which lifecycle phase focuses on evaluating control effectiveness and identifying gaps?
    - **A.** Initiation
    - **B.** Design
    - **C.** Monitoring
    - **D.** Implementation

Answers to Review Questions

1. B. Privacy governance establishes the framework through which an organization manages personal information in alignment with its strategic objectives, regulatory obligations, and stakeholder expectations. It defines roles, policies, and oversight mechanisms to ensure that privacy is consistently addressed across the enterprise. It does not eliminate all risk; instead, it ensures that risks are identified, managed, and monitored appropriately.
2. C. Personal information encompasses any data that can directly or indirectly identify an individual, including names, identifiers, location data, and behavioral attributes. It is broader than just sensitive categories such as financial or medical records. It includes any information that can reasonably be associated with a person, either alone or in combination with other data.
3. D. GDPR specifies six lawful bases for processing personal data: consent, contract, legal obligation, vital interests, public task, and legitimate interests. Business convenience is not recognized as a lawful basis, emphasizing that organizations must justify processing with clearly defined legal grounds rather than operational preference or efficiency.
4. B. Purpose limitation requires organizations to define and document the specific purposes for which personal data is collected and to ensure that data is not used in ways incompatible with those purposes. This principle prevents function creep and helps maintain trust by ensuring that individuals' data is not repurposed without appropriate justification.
5. C. The first line of defense consists of business and operational teams that handle personal information in their daily activities. These teams are responsible for implementing privacy controls, adhering to policies, and managing risks across their processes. They are accountable for ensuring that personal data is handled appropriately at the point of use.

6. B. Valid consent under the GDPR must be freely given, specific, informed, and unambiguous, and, in some cases, explicit. It must also be revocable at any time. Consent cannot be assumed through silence or inactivity, and it is only one of several lawful bases for processing, not a universal requirement.

7. C. The second line of defense includes privacy, compliance, and risk management functions that define policies, provide guidance, and monitor adherence to requirements. They support the first line by interpreting regulations, advising on risks, and ensuring that controls are appropriately designed and functioning.

8. C. A privacy notice, also known as a notice of privacy practices (NOPP), informs individuals about how their personal information is collected, used, shared, and protected. It is a key mechanism for transparency and is often legally required. It differs from internal documents in that it focuses on external communication with data subjects.

9. C. Privacy by design requires that privacy considerations be incorporated into systems, processes, and products from the outset, rather than added later. This proactive approach reduces risk, improves compliance, and ensures that privacy protections are integral to how systems operate.

10. C. Data minimization limits the collection, use, and retention of personal data to what is strictly necessary to achieve a defined purpose. This reduces exposure, lowers risk, and supports compliance with regulatory requirements that discourage excessive data collection.

11. B. A risk register is a structured record of identified risks, their likelihood and impact, and the decisions made to mitigate or accept them. In a privacy context, it helps ensure that risks to individuals are systematically identified, evaluated, and managed over time.

12. B. Transparency involves clearly informing individuals about how their personal data is collected, used, and shared. A privacy notice is a primary tool for achieving transparency, enabling individuals to understand and exercise their rights.

13. C. Internal audit serves as the third line of defense and provides independent assurance that governance, risk management, and control processes are effective. It evaluates whether privacy controls are properly designed and operating as intended.

14. A. A legal basis under GDPR is the lawful justification for processing personal data. Organizations must identify and document a valid legal basis before processing, ensuring that the activity is permitted under the regulation.

15. B. A DPIA is a structured process used to identify, assess, and mitigate risks to individuals arising from data processing activities, particularly those that are high risk. It supports compliance and helps organizations proactively address privacy concerns.

16. B. Accountability requires organizations not only to comply with privacy requirements but also to demonstrate that compliance through documentation, controls, and evidence. This includes maintaining records, conducting assessments, and showing that appropriate governance is in place.

17. C. The California Privacy Rights Act (CPRA) expanded the CCPA by introducing the concept of Sensitive Personal Information (SPI), which includes categories such as precise geolocation data and financial data. It also provides additional rights to limit the use of such information.

18. B. Privacy documentation, including policies, procedures, and records, ensures consistent practices and provides evidence of compliance. It supports governance, facilitates audits, and helps organizations demonstrate accountability.

19. B. Data consists of raw values or observations, while information is created when data is processed and interpreted within a context. This distinction is important because privacy obligations typically apply to meaningful information about individuals.

20. C. The monitoring phase involves assessing the performance and effectiveness of privacy controls through metrics, audits, and reviews. It identifies gaps, weaknesses, and areas for improvement, enabling the organization to maintain compliance and strengthen its privacy program over time.