Chapter 1

Developing a Privacy Program

THE CIPM EXAM OBJECTIVES COVERED IN THIS CHAPTER INCLUDE:

✓ **Domain I. Developing a Privacy Program**

- I.A. Create an organizational vision
  - I.A.a. Evaluate the intended objective
  - I.A.b. Gain executive sponsor approval for this vision
- I.B. Establish a data governance model
  - I.B.a. Centralized
  - I.B.b. Distributed
  - I.B.c. Hybrid
- I.C. Define a privacy program
  - I.C.a. Define program scope and charter
  - I.C.b. Identify the source, types, and uses of personal information (PI) within the organization and the applicable laws.
  - I.C.c. Develop a privacy strategy
- I.D. Structure the privacy team
  - I.D.a. Establish the organizational model, responsibilities, and reporting structure appropriate to the size of the organization (e.g., Chief Privacy Officer, DPO, Privacy manager, Privacy analysts, Privacy champions, "First responders")
  - I.D.b. Designate a point of contact for privacy issues
  - I.D.c. Establish/endorse the measurement of professional competency

- I.E. Communicate
  - I.E.a. Create awareness of the organization's privacy program internally and externally (e.g., PR, Corporate Communication, HR)
  - I.E.b. Develop internal and external communication plans to ingrain organizational accountability
  - I.E.c. Ensure employees have access to policies and procedures and updates relative to their role.

Organizations around the world find themselves under increasing scrutiny for their privacy practices. Legal and regulatory requirements, consumer pressure, and ethical obligations drive them to identify the personal information that they use and to implement controls to protect the privacy of that information.

As privacy functions flourish within organizations, they need qualified managers and leaders to ensure their success. From top-level chief privacy officers to mid-level managers, demand continues to increase for privacy experts.

Introduction to Privacy

Privacy is one of the core rights inherent to every human being. The term is defined in many historic works, but they all share the basic tenet of individuals having the right to protect themselves and their information from unwanted intrusions by others or the government. Let's take a brief look at the historical underpinnings of privacy in the United States.

In 1890, lawyers Samuel D. Warren and Louis D. Brandeis wrote an article for the *Harvard Law Review* titled "The Right to Privacy." In that article, they wrote:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right "to be let alone." Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.

Reading that excerpt over a century later, we can easily see echoes of Warren and Brandeis's concerns about technology in today's world. We could just as easily talk about the impact of social media, data brokerages, and electronic surveillance as having the potential to cause "what is whispered in the closet" to be "proclaimed from the house-tops."

The words written by Warren and Brandeis might have slipped into obscurity were it not for the fact that 25 years later one author would ascend to the Supreme Court where, as Justice Brandeis, he would take the concepts from this law review article and use them to argue

for a constitutional right to privacy. In a dissenting opinion in the case *Olmstead v. United States*, Justice Brandeis wrote:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness . . . . They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

This text, appearing in a dissenting opinion, was not binding upon the courts, but it has surfaced many times over the years in arguments establishing a right to privacy as that right "to be let alone." Recently, the 2018 majority opinion of the court in *Carpenter v. United States* cited *Olmstead* in an opinion declaring warrantless searches of cell phone location records unconstitutional, saying:

> As Justice Brandeis explained in his famous dissent, the Court is obligated as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, "after consulting the lessons of history," drafted the Fourth Amendment to prevent.

This is just one example of many historical precedents that firmly establish a right to privacy in U.S. law and allow the continued reinterpretation of that right in the context of technologies and tools that the authors of the Constitution could not possibly have imagined.

What Is Privacy?

It would certainly be difficult to start a book on privacy without first defining the word *privacy*, but this is a term that eludes a common definition in today's environment. Legal and privacy professionals asking this question often harken back to the words of Justice Brandeis, describing privacy simply as the right "to be let alone."

In their Generally Accepted Privacy Principles (GAPP), the American Institute of Certified Public Accountants (AICPA) offers a more hands-on definition, describing privacy as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information."

The GAPP definition may not be quite as pithy and elegant as Justice Brandeis's right "to be let alone," but it does provide privacy professionals with a better working definition that they can use to guide their privacy programs, so it is the definition that we will adopt in this book.

What Is Personal Information?

Now that we have privacy defined, we're led to another question. If privacy is about the protection of *personal information*, what information fits into this category? Here, we turn our attention once again to GAPP, which defines personal information as "information that is or can be about or related to an identifiable individual."

More simply, if information is about a person, that information is personal information as long as you can identify the person that it is about. For example, the fairly innocuous statement "Mike Chapple and Joe Shelley wrote this book" fits the definition of personal information. That personal information might fall into the public domain (after all, it's on the cover of this book!), but it remains personal information.

You'll often hear the term *personally identifiable information (PII)* used to describe personal information. The acronym PII is commonly used in privacy programs as a shorthand notation for all personal information.

Of course, not all personal information is in the public domain. Many other types of information fit into this category that most people would consider private. Our bank balances, medical records, college admissions test scores, and email communications are all personal information that we might hold sensitive. This information fits into the narrower category of *sensitive personal information (SPI)*. SPI tends to designate the type of information that a person might want to keep confidential. SPI can have differing levels of sensitivity and may also be protected by law. For example, General Data Protection Regulation (GDPR) in the European Union (EU) has a listing of "special categories of personal data," which includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data used for the purpose of uniquely identifying a natural person
- Health data
- Data concerning a natural person's sex life or sexual orientation

GDPR uses this list to create special boundaries and controls around the categories of information that EU lawmakers found to be the most sensitive.

What Isn't Personal Information?

With a working knowledge of personal information under our belts, it's also important to make sure that we have a clear understanding of what types of information do not fit the definition of personal information and, therefore, fall outside the scope of privacy programs.

First, clearly, if information is not about a person, it is not personal information. Information can be sensitive, but not personal. For example, a business's product development plans or a military unit's equipment list might both be very sensitive but they aren't about people, so they don't fit the definition of personal information.

Second, information is not personal information if it does not provide a way to identify the person that the information is about. For example, consider the height and weight information in Table 1.1.

TABLE 1.1 Height and weight information

Name	Age	Gender	Height	Weight
Mary Smith	43	F	5′ 9″	143 lbs
Matt Jones	45	M	5′ 11″	224 lbs
Kevin Reynolds	32	M	5′ 10″	176 lbs

This information clearly fits the definition of personal information. But what if we remove the names from this table, as shown in Table 1.2?

TABLE 1.2 Deidentified height and weight information

Age	Gender	Height	Weight
43	F	5′ 9″	143 lbs
45	M	5′ 11″	224 lbs
32	M	5′ 10″	176 lbs

Here, we have a set of information (or attributes) that are about an individual, but it doesn't seem to be about an *identifiable* individual, making the information *deidentified* and falling outside the definition of personal information. However, we must be careful here. What if this table was known to be the information about individuals in a certain department? If Mary Smith is the only 43-year-old female in that department, it would be trivial to determine that the first row contains her personal information, making the height and weight information once again identifiable information.

This leads us to the concept of *anonymization*, the process of taking personal information and making it impossible to identify the individual to whom the information relates. As illustrated in our height and weight example, simply removing names from a table of data

does not necessarily anonymize that data. Anonymized data should never be related back to a specific individual, and the anonymization process is actually a quite challenging problem and requires the expertise of privacy professionals.

Exam Tip

It's important to understand that deidentification and anonymization are similar, but not identical, concepts. Deidentification is the removal of identifying characteristics from data, as was done in Table 1.2. Anonymization is the process of altering information to a point that makes it impossible to tie it back to a specific individual person.

The U.S. Department of Health and Human Services (HHS) publishes a deidentification standard that may be used to render information unidentifiable using two different techniques:

The HHS deidentification standards cover medical records, so they include fields specific to medical records. You may use them as general guidance for the deidentification of other types of record, but you must also supplement them with industry-specific fields that might identify an individual. You can read the full HHS deidentification standard at www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard.

- *Expert determination* requires the involvement of a trained statistician who analyzes a deidentified data set and determines that very little risk exists that the information could be used to identify an individual, even if that information is combined with other publicly available information.
- *Safe harbor* requires the removal of 18 different types of information and indirect links to an individual. These include:
  - Names
  - Geographic divisions and ZIP codes containing fewer than 20,000 people
  - The month and day of a person's birth, death, and hospital admission or discharge or the age in years of a person over 89
  - Telephone numbers
  - Vehicle identifiers and serial numbers, including license plate numbers
  - Fax numbers
  - Device identifiers and serial numbers
  - Email addresses

- Web URLs
- Social Security numbers
- IP addresses
- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other uniquely identifying number, characteristic, or code
- Certificate/license numbers

We will cover how this standard fits into the broader requirements of the Health Insurance Portability and Accountability Act (HIPAA) in Chapter 2, "Privacy Program Framework." We only discuss it here as an example of the difficulty of deidentifying personal information.

Closely related to issues of anonymization and deidentification is the process of *aggregation*, summarizing data about a group of individuals in a manner that makes it impossible to draw conclusions about a single person. For example, we might survey all the students at a university and ask them their height and weight. If the students included any identifying information on their survey responses, those individual responses are clearly personal information. However, if we provide the summary table shown in Table 1.3, the information has been aggregated to an extent that renders it nonpersonal information. There is no way to determine the height or weight of an individual student from this data.

TABLE 1.3 Aggregated height and weight information

Gender	Average Height	Average Weight
F	5′ 5″	133 lbs
M	5′ 10″	152 lbs

Why Should We Care about Privacy?

Protecting privacy is hard work. Privacy programs require that organizations invest time and money in an effort that does not necessarily provide a direct financial return on that investment. This creates an opportunity cost, as those resources could easily be deployed in other areas of the organization to have a direct financial impact on the mission. Why, then, should organizations care about privacy?

Privacy is an ethical obligation. Organizations who are the custodians of personal information have a moral and ethical obligation to protect that information against unauthorized disclosure or use.

Laws and regulations require privacy protections. Depending on the nature of an organization's operations and the jurisdiction(s) where it operates, they may face legal and contractual obligations to protect privacy. Much of this book is dedicated to exploring these obligations.

Poor privacy practices reflect poorly on an organization. The failure to protect privacy presents a reputational risk to the organization, which may suddenly find its poor privacy practices covered on the front page of the *Wall Street Journal*. The reputational impact of a privacy lapse may have a lasting impact on the organization.

Consumers demand strong privacy practices. Today's consumer is increasingly sophisticated and aware of privacy concerns. The modern consumer expects organizations to take appropriate steps to protect their personal information and to transparently disclose their privacy practices.

Emerging technologies create new privacy concerns. The age of artificial intelligence (AI) and cloud computing creates many new opportunities to collect, store, and process personal information. These practices create new privacy issues that organizations adopting emerging technologies must address.

As the field of privacy matures, different organizations play a role in promoting strong privacy practices. The International Association of Privacy Professionals (IAPP) plays a strong role in developing and certifying privacy experts. Other organizations, including the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center (EPIC), advocate for strong privacy practices and appropriate applications of those practices to emerging technologies.

Generally Accepted Privacy Principles

Now that you have a basic understanding of the types of information covered by a privacy program and the reasons that organizations pay particular attention to protecting the privacy of personal information, we can start to explore the specific goals of a privacy program. These goals answer the question "What do we need to do to protect privacy?"

The *Generally Accepted Privacy Principles (GAPP)* are an attempt to establish a global framework for privacy management. GAPP includes 10 principles that were developed as a joint effort between two national accounting organizations: AICPA and the Canadian

Institute of Chartered Accountants (CICA). These two organizations sought expert input to develop a set of commonly accepted privacy principles.

The 10 GAPP principles are:

1. Management
2. Notice
3. Choice and Consent
4. Collection
5. Use, Retention, and Disposal
6. Access
7. Disclosure to Third Parties
8. Security for Privacy
9. Quality
10. Monitoring and Enforcement

The remainder of this section explores each of these principles in more detail.

Exam Tip

GAPP is one of many frameworks designed to help privacy professionals articulate the goals of their privacy programs and industry best practices. Other similar frameworks include the Fair Information Practice Principles (FIPPs) and the Organisation for Economic Co-operation and Development's (OECD) Privacy Guidelines.

We present GAPP to you in this chapter as a framework to help you understand the basic requirements of privacy programs. The GAPP principles are not included in the CIPM/US exam objectives, so you shouldn't see exam questions specifically covering them.

You will see many of these principles come up repeatedly in federal, state, and international laws that *are* covered by the exam objectives, so expect to see questions covering these concepts, just not in the context of GAPP.

Management

Management is the first of the 10 privacy principles, and GAPP defines it as follows: "The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures." GAPP lists a set of criteria that organizations should follow to establish control over the management of their privacy program.

These criteria include:

- Creating written privacy policies and communicating those policies to personnel
- Assigning responsibility and accountability for those policies to a person or team
- Establishing procedures for the review and approval of privacy policies and changes to those policies
- Ensuring that privacy policies are consistent with applicable laws and regulations
- Performing privacy risk assessments on at least an annual basis
- Ensuring that contractual obligations to customers, vendors, and partners are consistent with privacy policies
- Assessing privacy risks when implementing or changing technology infrastructure
- Creating and maintaining a privacy incident management process
- Conducting privacy awareness and training and establishing qualifications for employees with privacy responsibilities

Notice

The second GAPP principle, *notice*, requires that organizations inform individuals about their privacy practices. GAPP defines notice as follows: "The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed."

The notice principle incorporates the following criteria:

- Including notice practices in the organization's privacy policies
- Notifying individuals about the purpose of collecting personal information and the organization's policies surrounding the other GAPP principles
- Providing notice to individuals at the time of data collection, when policies and procedures change, and when the organization intends to use information for new purposes not disclosed in earlier notices
- Writing privacy notices in plain and simple language and posting it conspicuously

Choice and Consent

Choice and consent is the third GAPP principle, allowing individuals to retain control over the use of their personal information. GAPP defines choice and consent as follows: "The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information."

The criteria associated with the principle of choice and consent are as follows:

- Including choice and consent practices in the organization's privacy policies
- Informing individuals about the choice and consent options available to them and the consequences of refusing to provide personal information or withdrawing consent to use personal information

- Obtaining implicit or explicit consent at or before the time that personal information is collected
- Notifying individuals of proposed new uses for previously collected information and obtaining additional consent for those new uses
- Obtaining direct explicit consent from individuals when the organization collects, uses, or discloses sensitive personal information
- Obtaining consent before transferring personal information to or from an individual's computer or device

Collection

The principle of *collection* governs the ways that organizations come into the possession of personal information. GAPP defines this principle as follows: "The entity collects personal information only for the purposes identified in the notice."

The criteria associated with the collection principle are:

- Including collection practices in the organization's privacy policies
- Informing individuals that their personal information will only be collected for identified purposes
- Including details on the methods used to collect data and the types of data collected in the organization's privacy notice
- Collecting information using fair and lawful means and only for the purposes identified in the privacy notice
- Confirming that any third parties who provide the organization with personal information have collected it fairly and lawfully and that the information is reliable
- Informing individuals if the organization obtains additional information about them

While it is not explicitly included in the collection criteria, data minimization is another crucial component of privacy programs. This principle says that an organization should collect the minimum amount of personal information necessary to meet their objectives and discard that information when it is no longer needed for that purpose.

Use, Retention, and Disposal

Organizations must maintain the privacy of personal information throughout its life cycle. That's where the principle of *use, retention, and disposal* plays an important role. GAPP defines this principle as follows: "The entity limits the use of personal information to the

purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information."

The criteria associated with the use, retention, and disposal principle are as follows:

- Including collection practices in the organization's privacy policies
- Informing individuals that their personal information will only be used for disclosed purposes for which the organization has obtained consent and then abiding by that statement
- Informing individuals that their data will be retained for no longer than necessary and then abiding by that statement
- Informing individuals that information that is no longer needed will be disposed of securely and then abiding by that statement

Access

One of the core elements of individual privacy is the belief that individuals should have the right to access information that an organization holds about them and, when necessary, to correct that information. This right to correct information is also known as the right of redress. The GAPP definition of the *access* principle is as follows: "The entity provides individuals with access to their personal information for review and update."

The criteria associated with the access principle are as follows:

- Including practices around access to personal information in the organization's privacy policies
- Informing individuals about the procedures for reviewing, updating, and correcting their personal information
- Providing individuals with a mechanism to determine whether the organization maintains personal information about them and to review any such information
- Authenticating an individual's identity before providing them with access to personal information
- Providing access to information in an understandable format within a reasonable period of time and either for a reasonable charge that is based on the organization's actual costs or at no cost
- Informing individuals in writing why any requests to access or update personal information were denied and informing them of any appeal rights they may have
- Providing a mechanism for individuals to update or correct personal information and providing that updated information to third parties who received it from the organization

Disclosure to Third Parties

Some challenging privacy issues arise when organizations maintain personal information about an individual and then choose to share that information with third parties in the course of doing business. GAPP defines the *disclosure to third parties* principle as follows: "The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual."

The criteria associated with the disclosure to third parties principle are as follows:

- Including third-party disclosure practices in the organization's privacy policies
- Informing individuals of any third-party disclosures that take place and the purpose of those disclosures
- Informing third parties who receive personal information from the organization that they must comply with the organization's privacy policy and handling practices
- Disclosing personal information to third parties without notice or for purposes other than those disclosed in the notice only when required to do so by law
- Disclosing information to third parties only under the auspices of an agreement that the third party will protect the information consistent with the organization's privacy policy
- Implementing procedures designed to verify that the privacy controls of third parties receiving personal information from the organization are functioning effectively
- Taking remedial action when the organization learns that a third party has mishandled personal information shared by the organization

Security for Privacy

Protecting the security of personal information is deeply entwined with protecting the privacy of that information. Organizations can't provide individuals with assurances about the handling of personal data if they can't protect that information from unauthorized access. GAPP defines *security for privacy* as follows: "The entity protects personal information against unauthorized access (both physical and logical)."

The criteria associated with the security for privacy principle are as follows:

- Including security practices in the organization's privacy policies
- Informing individuals that the organization takes precautions to protect the privacy of their personal information
- Developing, documenting, and implementing an information security program that addresses the major privacy-related areas of security listed in ISO 27002:
  - Risk assessment and treatment
  - Security policy
  - Organization of information security
  - Asset management
  - Human resources security

- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

This list includes the ISO 27002 elements that are relevant to privacy efforts and, therefore, our conversation. ISO 27002 does include other recommended security controls that fall outside the scope of a privacy effort.

- Restricting logical access to personal information through the use of strong identification, authentication, and authorization practices
- Restricting physical access to personal information through the use of physical security controls
- Protecting personal information from accidental disclosure due to natural disasters and other environmental hazards
- Applying strong encryption to any personal information that is transmitted over public networks
- Avoiding the storage of personal information on portable media, unless absolutely necessary, and using encryption to protect any personal information that must be stored on portable media
- Conducting periodic tests of security safeguards used to protect personal information

Quality

When we think about the issues associated with protecting the privacy of personal information, we often first think about issues related to the proper collection and use of that information along with potential unauthorized disclosure of that information. However, it's also important to consider the accuracy of that information. Individuals may be damaged by incorrect information just as much, if not more, than they might be damaged by information that is improperly handled. The GAPP *quality* principle states that "The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice." The quality principle enforces data integrity.

The criteria associated with the quality principle are as follows:

- Including data quality practices in the organization's privacy policies

- Informing individuals that they bear responsibility for providing the organization with accurate and complete personal information and informing the organization if corrections are required
- Maintaining personal information that is accurate, complete, and relevant for the purposes for which it will be used

Monitoring and Enforcement

Privacy programs are not a one-time project. It's true that organizations may make a substantial initial investment of time and energy to build up their privacy practices, but those practices must be monitored over time to ensure that they continue to operate effectively and meet the organization's privacy obligations as business needs and information practices evolve. The GAPP *monitoring and enforcement* principle states that "The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquires, complaints, and disputes."

The criteria associated with the monitoring and enforcement principle are as follows:

- Including monitoring and enforcement practices in the organization's privacy policies
- Informing individuals about how they should contact the organization if they have questions, complaints, or disputes regarding privacy practices
- Maintaining a dispute resolution process that ensures that every complaint is addressed and that the individual who raised the complaint is provided with a documented response
- Reviewing compliance with privacy policies, procedures, laws, regulations, and contractual obligations on an annual basis
- Developing and implementing remediation plans for any issues identified during privacy compliance reviews
- Documenting cases where privacy policies were violated and taking any necessary corrective action
- Performing ongoing monitoring of the privacy program based on a risk assessment

Developing a Privacy Program

At this point in the chapter, you should have a reasonable understanding of the fact that privacy issues are complex and nuanced. There are no "quick fix" solutions to protecting the privacy of personal information, and organizations developing a privacy program for the first time will need to expend considerable effort designing that program, implementing appropriate privacy controls, and monitoring the program's ongoing effectiveness to ensure that it continues to meet the organization's legal obligations and privacy objectives.

Crafting Vision, Strategy, Goals, and Objectives

At the outset of a privacy initiative, senior leadership should outline the vision, strategy, and goals of the privacy program. These provide the high-level direction that those implementing the program will need to guide their efforts. For example, the U.S. Department of Commerce (DOC) offers the following mission statement for their privacy program:

> The DOC is committed to safeguarding personal privacy. Individual trust in the privacy and security of personally identifiable information is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on millions of individuals and companies, the developer of information management standards and a federal advisor on information management policy, the Department strives to be a leader in best privacy practices and privacy policy. To further this goal, the Department assigns a high priority to privacy consideration in all systems, programs, and policies.

That's a very high-level statement that clearly explains the purpose of the program. Notice that it doesn't contain any specific objectives or measures. The privacy obligations and controls used by the DOC might change over time, but it is very likely that this strategic-level mission statement will remain appropriate (at least through the end of the 21st century!). The program document also contains goals that the DOC has to guide the execution of a privacy program in support of their mission. The four goals of their plan are as follows:

1. Foster a culture of privacy and disclosure and demonstrate leadership through policy and partnerships.
2. Provide outreach, education, training, and reports in order to promote privacy and transparency.
3. Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all DOC activities.
4. Develop and maintain the best privacy and disclosure professionals in the federal government.

These goals start to get into the details of *how* the DOC will carry out its privacy mission. They provide four key deliverables that privacy officials can then use to align their work with the DOC's strategy.

Beneath each of these goals, the DOC provides a series of specific objectives that will satisfy each goal. These are the activities that the DOC plans to undertake to meet its goal and, therefore, achieve the privacy program's strategic purpose. For brevity's sake, we won't cover all the objectives in this book, but let's take a look at the four objectives that align with the DOC's third privacy goal to conduct robust compliance and oversight programs:

1. Review, assess, and provide guidance to DOC programs, systems, projects, information sharing arrangements, and other initiatives to reduce the impact on privacy and ensure compliance.

2. Promote privacy best practices and guidance to the DOC's information sharing and intelligence activities.
3. Ensure that complaints and incidents at DOC are reported systematically, processed efficiently, and mitigated appropriately in accordance with federal and DOC privacy policies and procedures.
4. Evaluate DOC programs and activities for compliance with privacy and disclosure laws.

These objectives are highly specific, and you might imagine them being handed to a middle manager to execute. They also might change much more frequently than the program's high-level purpose in order to meet the changing needs of the DOC.

Throughout this section, we draw examples from the Department of Commerce's Privacy Plan. If you'd like to review this plan in more detail, you can download it from `http://osec.doc.gov/opog/privacy/Memorandums/PRIVACY_PROGRAM_PLAN_2017.pdf`.

Obtaining Executive Support

The privacy program will require resources to succeed. Those resources include the time of privacy team members and other stakeholders throughout the organization, funds to cover the direct costs of the program, and authority to enforce new policy directions. Therefore, it's crucial that the privacy program have executive-level support.

The best way for a new program to obtain this support is to have an executive sponsor who will serve as the program's champion with the organization's leadership. The executive sponsor should agree with the vision and strategy for the privacy program, and it is crucial to gain that person's approval before moving forward.

Ensure Business Alignment

While privacy professionals find themselves primarily focused on the world of privacy, they must also remember that they are part of a larger organization with a different mission. The purpose of the organization might be to create software, educate students, govern a nation, or almost anything else imaginable. In order for a privacy program to succeed, it must be able to justify its existence within the context of that broader mission.

This leads to one of the key responsibilities of a privacy manager: ensuring that the privacy program remains aligned with the broader business. It's easy for privacy experts to get lost in the weeds of their work and come to think of privacy as an end in and of itself, but privacy is only effective when it facilitates the achievement of organizational goals and objectives. Privacy efforts must align with the business's goals, objectives, functions, processes, and practices.

There are five key ways that privacy managers can ensure this business alignment:

Finalize the business case for privacy. Privacy managers must be able to justify the investments of time and money that they expect the organization to make in the privacy program. This requires identifying how privacy supports business goals and clearly articulating the return on investment that senior leaders should expect.

Identify stakeholders. There are many different stakeholders who play a role in achieving the objectives of a privacy program. These include information security, human resources, marketing, legal, procurement, and other specialists. It's important to bring these stakeholders into the process early and engage them in the privacy program. You'll learn more about effective ways to integrate these business functions with the privacy program in Chapter 4, "Privacy Operational Life Cycle: Protect."

Leverage key functions. In addition to involving other business functions as stakeholders in the privacy program, privacy managers should leverage the expertise of those functions to achieve privacy objectives. For example, privacy professionals spend much of their time analyzing and interpreting legal requirements. The organization's legal team can play an invaluable role assisting with this work. Similarly, most organizations have communications teams that can assist with communicating privacy messages.

Create a process for interfacing within the organization. The privacy team will often work closely with other teams in the organization and should have clearly defined processes for these interactions. For example, the information technology team will likely have to carry out much of the technical work of the privacy program. Privacy professionals should understand the IT service management (ITSM) processes used by that team and take advantage of that knowledge to improve their ability to work together.

Align organizational culture and privacy/data protection objectives. Every organization has a unique culture, and navigating that culture is crucial to the success of internal initiatives. Privacy professionals should understand the culture of their organization and use that knowledge to successfully advance privacy objectives.

Developing Business Cases

The implementation and management of privacy personnel, projects, and tools requires investments of financial and human resources by the organization. Those resources are, of course, finite, and there is normally stiff competition within the organization over their allocation. Other business leaders may want the same resources assigned to initiatives they find to be a higher priority, whereas shareholders may prefer that the resources be returned to them as profit in the form of dividends.

Therefore, privacy managers must be able to make coherent business cases that justify their proposed investments. These business cases outline the rationale for the investment and justify it as the best possible use of the requested resources. Privacy managers should investigate the business case process used by the rest of their organization and adopt it as closely as possible. These formats may vary, but they typically include several core components:

A *scope statement* that concisely describes the proposed initiative

The *strategic context* that demonstrates the need for the initiative and how the investment aligns with the organization's broader strategic goals

A *cost analysis* that outlines the financial and human resource costs of the initiative, on both a one-time and a recurring basis

An *evaluation of alternatives* that describes other possible approaches for achieving the strategic goals addressed by this project and explains why the current proposal is the best available option

A *project plan* that describes the detailed implementation plan for the initiative

A *management plan* that describes how the organization will oversee the processes created by this initiative on an ongoing basis in a manner that integrates with the privacy and corporate governance frameworks

Maintain Flexibility

Privacy programs have clearly stated objectives, but at the same time, managers must ensure that the program remains flexible enough to accommodate changing requirements. Leaders must monitor legislative, regulatory, market, and business requirements to ensure that the program remains relevant.

This flexibility should extend to all aspects of your privacy strategy. For example, you may need to adapt your privacy strategy to accommodate different regulatory requirements, business needs, and the cultural norms of the geographic areas where your business operates.

Structuring the Privacy Team

Organizations should appoint a senior leader with overall responsibility for the organization's privacy program. This establishes senior-level accountability for the program's success and provides the privacy program with a seat at the executive table. This role is commonly referred to as an organization's *chief privacy officer (CPO)*, although it may also be implemented using other titles, such as director of privacy or privacy program manager. The CPO also serves as the designated point of contact in the organization for privacy issues, although they may delegate much of the responsibility for handling those issues to privacy analysts or others on their team.

Ethics Officers

Many organizations now have dedicated ethics officers, and in fact, some regulations now require the creation of this office. Ethics officers should work closely with privacy teams to ensure that the organization meets its privacy obligations and acts in a responsible manner. An organization's ethics officer typically has a reporting relationship with the board of directors, allowing them to communicate directly with the board when issues arise that affect senior leadership.

In the DOC Privacy Plan that we have been using as an example in this section, the department identifies a position within the office of the Secretary of Commerce as the DOC's chief privacy officer. The program includes a detailed set of responsibilities for this position. Here is an abbreviated set of those responsibilities, paraphrased for brevity:

- Serve as the senior privacy policy authority
- Develop and oversee implementation of privacy policies
- Communicate the privacy vision, principles, and policy internally and externally
- Ensure the department complies with applicable privacy laws and regulations
- Advocate privacy-preserving strategies for information collection and dissemination
- Manage privacy risks
- Ensure employees and contractors receive appropriate privacy training
- Facilitate relationships with senior DOC leaders, other federal agencies, and private industry

Of course, the DOC is a very large organization and it would be impossible for one person to be involved in all aspects of its privacy program in any type of thorough manner. For this reason, the DOC policy also specifies that each operating unit should have its own CPO and that those CPOs should meet regularly as the Department of Commerce Privacy Council.

This type of hierarchical privacy authority is common in government agencies and other large organizations. It may not be necessary in smaller organizations, depending on the nature of the organization and the scope of its privacy program. Some organizations opt to use the role of "privacy champions" distributed throughout the organization. These liaisons serve as the primary point of privacy contact for their organization and work directly with the CPO office. Depending on the size of the unit they serve, the liaison role may be a full-time position or a secondary responsibility for someone in another primary role.

The composition and structure of the privacy team will vary depending on the size of the organization and the complexity of its privacy requirements. In smaller organizations, a single individual might be appointed as the data protection officer (DPO) for GDPR compliance purposes and also be responsible for the management of the entire privacy program. Larger organizations may have a large team consisting of a CPO, a DPO, several privacy managers, and teams of privacy analysts and first responders who handle emerging privacy incidents.

Measuring Professional Competency

Privacy is a professional discipline, and it is important that privacy leaders take steps to establish and endorse the measurement of professional competency. One of the primary mechanisms they may use to achieve this goal is providing team members with the encouragement and resources necessary to obtain privacy certifications appropriate to their goals. This may include having privacy team members earn the Certified Information Privacy Professional (CIPP) certification(s) appropriate for the regions where they operate and having IT professionals who work on privacy initiatives earn the Certified Information Privacy Technologist (CIPT) credential.

The reporting structure for privacy leaders also varies from organization to organization, and the choice of reporting structure conveys a message about the importance that the organization places on privacy. For example, organizations where the CPO reports directly to the chief executive officer (CEO) may convey the message that they take privacy more seriously than an organization where the CPO reports to the general counsel or chief risk officer.

Creating a Program Scope and Charter

New privacy managers in an organization without a mature privacy function may find themselves developing a program from the ground up. This effort should begin with the development of a privacy strategy that outlines the vision, mission, goals, and objectives of the program.

With that strategy in hand, managers may begin to outline the set of initiatives required to bring the organization from its current state to the desired state of privacy. As they establish the program, they should ensure that its work remains aligned with the privacy strategy that guides their effort.

Defining Program Scope

The first step in developing a new privacy program is creating a clear statement of the program's *scope*. This is the definition of the activities that are (and are not) included in the program's work. There are two important elements to the program's scope:

The Type of Privacy Objectives Included in the Program Does the program cover all aspects of privacy, or are there exceptions? For example, does the privacy program cover international requirements, or is it specific to one jurisdiction?

The Portion of the Organization Covered by the Privacy Program A privacy program might cover the entire organization, or its work might be limited to a business unit or other portion of the organizational structure.

In most cases, the scope statement may be concise, communicating the nature of the program clearly to all employees. For example, a broadly defined privacy program might use this scope statement:

> The privacy program is responsible for protecting the privacy of all personally identifiable information stored, processed, or transmitted by the organization in any form: physical or digital.

If the program applies only to a specific area of the organization or excludes a specific area of the organization, this would also be included in the scope statement. For example, many universities have associated health systems and those health systems often have separate privacy functions. In that situation, the university's main privacy program might have a scope statement that describes this scope limitation:

> The privacy program is responsible for protecting the privacy of all personally identifiable information stored, processed, or transmitted by the organization in any form: physical or digital. The program does not apply to elements of the University Health System governed by the UHS Privacy Program.

Developing a Program Charter

With a scope statement in hand, privacy managers may then begin creating the privacy program *charter*. The charter is the organizing document for the privacy program. Building on the scope, the charter outlines the parameters within which the program will function. Common components of a privacy program charter include the following:

- *A scope statement* identifying the scope of the privacy program. This is simply reiterating the scope statement created for the program in a location where all interested stakeholders may reference it.
- *A business purpose* clearly linking the privacy program objectives to business objectives. For example, the University of Pennsylvania uses this business purpose statement in their Information Security and Privacy Program Charter (`www.isc.upenn.edu/information-security-and-privacy-program-charter`):

  > Penn is committed to preeminence in research, teaching, and service. As a result, Penn owns significant assets in the form of information. Penn's informational assets include, but are not limited to, student education records, employment records, financial information, research data, protected health information, alumni and donor information, Penn operational data, Penn intellectual property, and other data relating to Penn's infrastructure, technology resources, and information security. The improper use of such information, the unauthorized or inadvertent disclosure, alteration or destruction of information assets, or a significant interruption in their availability can disrupt Penn's ability to fulfill its mission. Such actions can also result in regulatory, legal, financial, and/or reputational risk to Penn and to the individuals whose data Penn maintains.

- *A statement of authority* for the program, normally delegating institutional authority to a specific individual. For example, a statement of authority might read:

  > The Chief Privacy Officer (CPO) is responsible for coordinating and overseeing the privacy program. The CPO may designate other representatives of the organization to oversee and coordinate portions of the program.

- *Roles and responsibilities* for other stakeholders who have the responsibility to help carry out the activities of the privacy program. This may include:
  - Senior leaders
  - Privacy team members
  - Security and other information technologists
  - Internal and external auditors
  - Data owners, stewards, and custodians
  - Other employees and stakeholders
- *Governance structure and processes* that will continue to ensure that the organization's privacy program remains in alignment with the organization's business goals
- *Program documentation procedures* that formalize how the organization will establish, communicate, and maintain privacy standards, guidelines, procedures, and other documentation
- *Enforcement mechanisms* that establish how the organization will guide and enforce compliance with privacy policies and provide consequences for individuals and units that fail to comply with privacy program requirements
- *A review process* that will be conducted on a periodic basis to ensure that the privacy program continues to achieve its objectives, that those objectives continue to align with business objectives, and that the privacy program is functioning properly
- *An approval statement* that clearly describes the authority under which the program is enacted. This is normally done through the signature of the CEO or other senior leader. This approval statement gives force to the delegation of authority and other details outlined in the charter.

The specific contents of any organization's privacy program charter will depend on the organization's business and privacy objectives, operational culture, and other factors. Rather than being overly concerned about the specific section headings included in a charter, privacy managers should ensure that the charter provides the framework under which they may effectively implement the program.

Privacy Roles

Depending on the nature of an individual's or organization's involvement in the collection and processing of information, they may take on one or more data roles. The three primary roles are as follows:

- *Data subjects* are the individuals about whom personal information is collected. These may be the customers or employees of an organization or any other individuals about whom the organization collects personal information.
- *Data controllers* are the organizations that determine the purposes and means of collecting personal information from data subjects. If an organization collects and/or processes personal information for its own business needs, it is a data controller. It remains a data controller even if it outsources some of that collection or processing to service providers.
- *Data processors* are service providers that collect or process personal information on behalf of data controllers. For example, cloud service providers often serve in the role of data processor for their customers.

These terms take on particular importance when interpreting how laws and regulations apply to an organization. For example, some regulations allow data controllers to transfer some privacy and security responsibility to service providers, as long as the controller chooses a service provider that has gone through a certification process. Regulations, including the EU's GDPR, may also have very specific definitions of these terms, as you will discover later in this book as we explore those regulations in more detail.

After clearly defining roles in an organization, privacy leaders should ensure that each individual receives training appropriate to their role and has access to the policies and procedures relevant to their role.

Building Inventories

Once an organization has established accountable officials and privacy roles, the next step in developing a privacy program is to create a comprehensive *data inventory* of the personal information that the organization collects, processes, and maintains and the systems, storage locations, and processes involved in those activities. The inventory provides a crucial starting point for privacy professionals seeking to understand the organization's privacy needs.

This inventory may take many different forms, depending on the nature of the organization and the level of formality desired. The end goal is for the organization to have a clear picture of the types of personal information that it handles, the sources of that information, and the ways that information is stored and processed. This inventory should be maintained as a living repository of data updated when business activities or privacy practices change or when there are shifts in the regulatory landscape that require tracking new elements of information. It may then be used as the basis for conducting privacy assessments and implementing privacy controls.

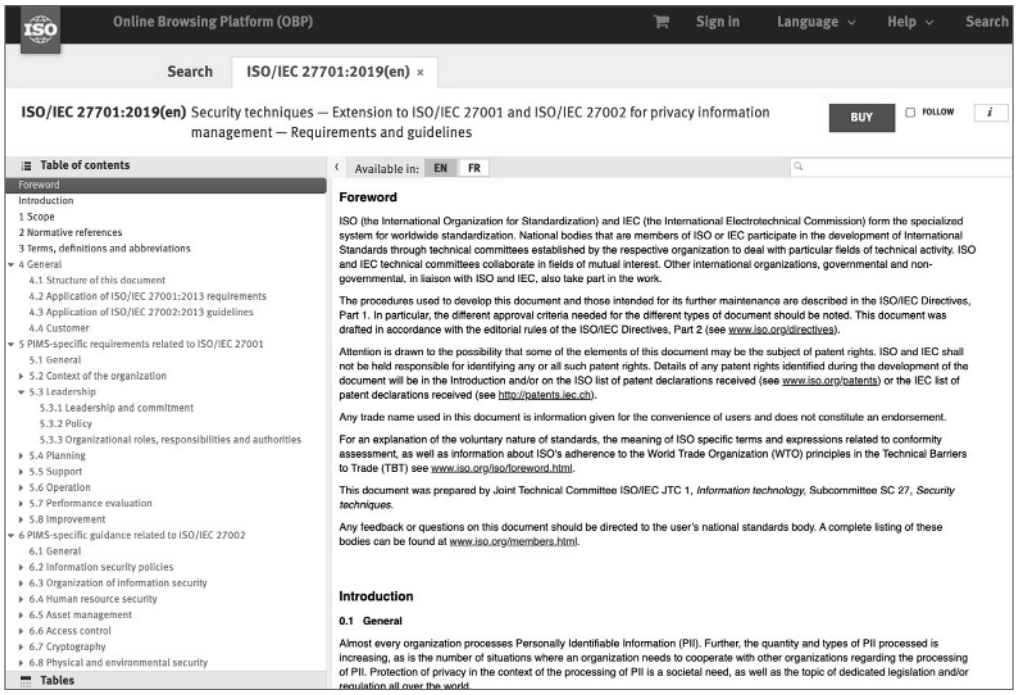
Information security programs also depend on a similar inventory of all sensitive information maintained by the organization. The personally identifiable information included in a privacy-focused inventory is a subset of that sensitive information inventory. This offers an excellent opportunity for privacy and information security programs to partner and avoid redundant activity by simply including a personal information tag in the broader sensitive information inventory.

Conducting a Privacy Assessment

With a personal information inventory in hand, the organization may now turn to an assessment of the current state of its privacy program. This assessment should use a standard set of privacy practices, derived from either an industry standard framework or the regulatory requirements facing the organization. The remainder of this book will dive deeply into many of these frameworks and requirements.

For example, an organization might choose to adopt the privacy framework from the International Organization for Standardization titled "Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines" and documented in ISO 27701. An excerpt from this document appears in Figure 1.1.

FIGURE 1.1 Excerpt from ISO 27701



ISO 27701 is closely linked to ISO 27001 and 27002, the two ISO standards governing information security. This is another opportunity to align the interests of privacy and security programs. Annex F of ISO 27701 provides advice on applying the privacy standard in an organization that already uses the information security standards. These standards are also tightly linked to the National Institute for Standards and Technology's Cybersecurity Framework (CSF), allowing organizations to cleanly map controls between standards and frameworks that they adopt for both privacy and security.

The end result of the privacy assessment should be a *gap analysis* that identifies any places where the organization's current practices do not meet the level of control desired by the standard under which the assessment was performed. This gap analysis may then be used in remediation efforts to bring the organization up to the desired level of privacy performance.

Implementing Privacy Controls

The primary means that the organization uses to remediate privacy deficiencies is the implementation of *privacy controls* that are technical or administrative measures that improve privacy. For example, implementing mechanisms that fulfill the many GAPP criteria discussed earlier in this chapter qualify as privacy controls. Here are some examples of common privacy controls:

- Creation, review, or modification of privacy policies
- Use of encryption to protect personal information
- Purging of personal information when it is no longer needed to meet the purposes disclosed when it was collected
- Configuring access controls to limit the use of personal information to authorized individuals
- Implementing and maintaining a process to manage user privacy preferences
- Developing a standard process for investigating privacy complaints and following up on potential privacy incidents
- Conducting periodic testing and assessment of the organization's privacy program

Notice that some, but not all, of these controls are technical in nature, but all the controls advance the organization's privacy efforts.

Ongoing Operation and Monitoring

Once a privacy program is well established, the organization should continue to operate the program and monitor its effectiveness. This is normally done through a combination of periodic reviews, regular updates to the privacy assessment, and dashboard-style monitoring of the program's key metrics, such as compliance with data retention and disposal standards, turnaround time for processing privacy requests, and the number and severity of privacy incidents.

Organizations may also find themselves the subject of *privacy audits* based on legal or regulatory requirements. Audits are similar to assessments in nature, because they compare the current state of the privacy program to an external standard. However, unlike assessments, audits are always performed by an independent auditor who does not have a vested interest in the outcome. Audits may be performed at the request of internal management, a board of directors, or regulatory authorities.

Data Governance

Data governance is the set of policies, procedures, and controls that an organization develops to safeguard its information while making it useful for transactional and analytic purposes. As the name implies, data governance is primarily a business function. Governments have a method for creating, interpreting, and enforcing laws. Part of this process ensures that these laws are known to the citizenry. For organizations, data governance is an umbrella term covering the creation, interpretation, and enforcement of data use. Data governance efforts are crucial to privacy programs because they provide a framework for identifying and regulating the use of personal information throughout an organization.

Organizations develop numerous policies to govern their data. These policies promote data quality, specify the use of data attributes, and define access to different data domains. Additional governance policies identify how to secure data, comply with regulations, protect data privacy, and deal with data over time. Just as countries enforce laws, organizations implement procedural and technical controls to comply with data governance standards.

Strong executive support is vital to any data governance effort. An organization invests a significant amount of time and resources to define, develop, implement, and control access to data. For data governance to succeed, all levels of an organization must appreciate the importance of well-governed data. While technology is a critical component to facilitating adherence to policies, an information technology organization can't drive data governance efforts on its own. You need executive support across the organization for data governance efforts to succeed.

Data Governance Approaches

Data governance programs may operate using one of three different approaches:

- **Centralized** data governance programs have a core office that directs the data governance efforts of the entire organization.
- **Distributed** data governance programs may have organization-wide standards, but each business unit creates its own data governance program that achieves those shared objectives.
- **Hybrid** data governance programs combine the centralized and distributed approaches, with a centralized office providing oversight and guidance to distributed teams who focus on particular business units.

Data Governance Roles

It takes multiple people fulfilling a variety of roles for data governance to thrive. A crucial concept relating to data governance is data stewardship. Stewardship denotes looking after something, like an organization or property. *Data stewardship* is the act of developing the policies and procedures for looking after an organization's data quality, security, privacy, and regulatory compliance. The most vital role for effective data stewardship is that of the organizational data steward. An *organizational data steward*, or *data steward*, is the person responsible for data stewardship.

The data steward is responsible for leading an organization's data governance activities. As the link between the technical and nontechnical divisions within an organization, a data steward works with many people, from senior leaders to individual technologists. To establish policies, a data steward works with various data owners.

A *data owner* is a senior business leader with overall responsibility for a specific data domain. A *data domain*, or *data subject area*, comprises data about a particular operational division within an organization. Finance, human resources, and the physical plant are all examples of operational divisions. Data owners work with the data steward to establish policies and procedures for their data domain.

In large, complex organizations, data owners may choose to delegate day-to-day governance activities to subject area data stewards. A *subject area data steward* works in the data owner's organization and understands the nuances that apply within that organizational unit. A subject area data steward works on behalf of their data owner to handle daily tasks. For example, processing access requests as people rotate in and out of roles is a responsibility a data owner may delegate to their subject area data steward. The need for subject area data stewards arises from the intricacies of different data domains. To implement data governance policies, data stewards work with data custodians.

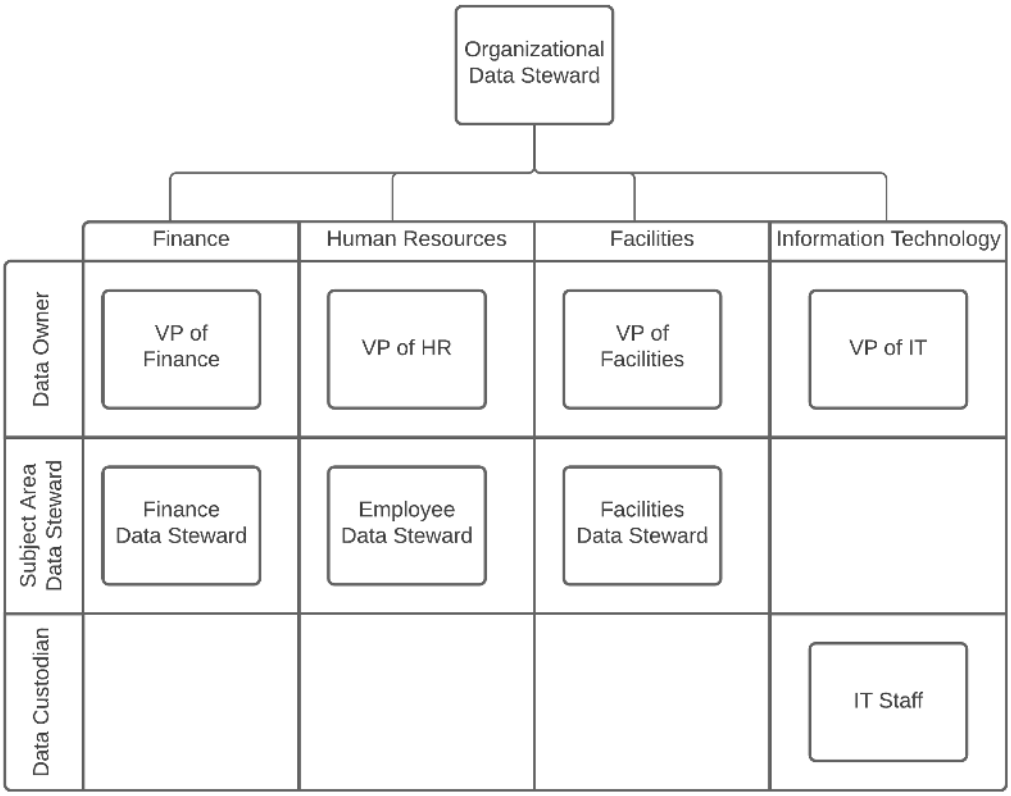
A *data custodian* is a role given to someone who implements technical controls that execute data governance policies. Data custodians are frequently information technology employees who configure applications, dashboards, and databases.

For example, unique laws govern an organization's finances, people, and physical plant. Figure 1.2 visualizes how an organizational data steward works both vertically and horizontally with the various data owners, subject area data stewards, and data custodians to actively steward, or take care of, the organization's data.

Access Requirements

One crucial component of data governance defines the access requirements for data. *Data access requirements* determine which people need access to what data. Access requirements differ by data subject area and can be as granular as a single field. For example, managers need access to details about their employees, including their names and contact information. Since managers are responsible for providing feedback, they also need access to performance data. However, no manager has a compelling need to view their employees' Social Security numbers (SSNs). Although SSNs are necessary for payroll and tax purposes, malicious actors can also use them for identity theft.

FIGURE 1.2 Organizational example



When determining access requirements, it is essential to develop a data classification matrix. A *data classification matrix* defines categories, descriptions, and disclosure implications for data. Table 1.4 is an example of a data classification matrix. It is vital to factor in data classification when considering access requirements to ensure proper data stewardship.

TABLE 1.4 Sample data classification matrix

Classification Term	Classification Description
Public	Data intended for public consumption—for example, anything on a public-facing website meets this classification. No disclosure implications.
Internal	Data intended for use within an organization—for example, a comprehensive organization chart including names. Disclosure compromises an organization's reputation or operations, but not its privacy or confidentiality obligations.

Classification Term	Classification Description
Sensitive	Data intended for limited use within an organization—for example, a list of employees and their compensation. Disclosure implies a violation of privacy or confidentiality.
Highly Sensitive	Data intended for restricted use, typically due to compliance obligations. Examples include Social Security numbers and bank account numbers. Disclosure implies a legal obligation in the event of a data breach.

A data steward works with a data owner to establish broad classifications, with subject area data stewards to develop procedures for granting access to information, and with data custodians to ensure the appropriate technical controls are in place to protect information.

Governing Information Processing

Data governance programs should provide oversight for all types of processing that the organization performs on personal information. This includes six core activities:

- **Collecting** personal information from individuals or other organizations
- **Using** personal information to achieve business objectives
- **Accessing** personal information by individual employees
- **Sharing** personal information internally and externally
- **Transferring** personal information internally and externally
- **Destroying** personal information when it is no longer necessary to meet business objectives

Managing the Privacy Budget

Privacy managers also have financial responsibility for their organization's privacy program. This means that they must participate in developing, implementing, and monitoring a budget.

Many privacy managers came up through the practitioner ranks and find themselves in their first management role, unfamiliar with many of the nontechnical skills required for the job. If that's your situation, you might find yourself unfamiliar with the skills and tools that can assist you with this task.

Organizational Budgeting

A *budget* is just a financial plan for the team. It outlines how much money is available to you over the course of the year and how you plan to spend that money.

Most organizations go through an annual budget planning cycle where the organization's leadership decides the following year's budget a few months before the year begins. This means that you'll have to work backward and will often find yourself preparing a budget at least six months in advance of it going into effect. Or, looking at it another way, depending on where you are in the budget cycle, it could be up to 18 months until the next time that you receive a budget adjustment. That's why planning in advance is so important.

The budgeting process is *extremely* important for privacy managers. Successfully completing the budgeting process is how you obtain the funding that you need for your privacy program and privacy team.

As you go through the budget planning process, you'll need to follow the guidelines set by your organization. There are two major approaches to budgeting:

- *Incremental budgeting* approaches start with the prior year's budget and then make adjustments by either raising or lowering the budget. If your organization uses this approach, you'll frequently hear phrases like "We have a 3 percent budget increase this year" or "We're cutting the budget by 5 percent." It's up to the manager to advocate for additional budget and to make the new numbers work.
- *Zero-based budgeting* approaches begin from zero each year and managers are asked to justify their entire budget, rather than starting with the assumption that they will have the same amount of funding as they did the previous year.

Expense Types

There are two different types of expenses in the world of business budgeting: capital expenses and operational expenses. If you've ever heard anyone using the phrase "different flavors of money," this is what they're talking about. Money that falls into the capital expense budget typically can't be used for operational expenses, and vice versa. Therefore, it's important to understand each type of money and how it may be used.

Capital expenses (CapEx) are costs that an organization incurs as part of building out and maintaining its large assets. For example, if you buy or renovate a building, that's a fixed asset, and the costs associated with it are capital expenses.

Other examples of capital expenses are:

- Purchasing expensive computing equipment
- Buying vehicles
- Buying new multifunction printers

Operational expenses (OpEx) are the costs of running the business day to day that don't involve purchasing or maintaining an asset. The most common example of operational expenses is payroll costs. You're paying your employees to run your business, but you're not purchasing the employee, so your employees are not a financial asset. This makes payroll an operational expense.

Other examples of operational expenses are:

- Electricity costs
- Hardware maintenance agreements
- Office supplies

The line between capital and operational expenses can be a little fuzzy and will depend on your organization's financial practices. Some organizations use a dollar threshold to help differentiate between the two, whereas others have more complex guidelines. You should check with your financial accounting team for help sorting this out.

Both capital and operating expenses may be one-time or recurring. For example, your privacy team's payroll is a recurring operational expense, whereas the cost of hiring a privacy consultant to conduct an assessment is likely treated as a one-time operational expense. Similarly, the building of a new data center is a one-time capital expense whereas the replacement of your servers is a recurring capital expense. Privacy programs will likely have a focus on operational, rather than capital, expenses due to the nature of the costs that they incur.

Capital expenses and operating expenses are treated very differently by tax laws and financial reporting regulations. That's the reason that accountants are so concerned with differentiating between the two and why it's difficult to move money between capital and operating budgets in some organizations.

Budget Monitoring

Budget planning is typically an annual chore that follows a very well-defined life cycle. However, a privacy manager's budget responsibility doesn't end once the planning cycle concludes. In fact, the work has only just begun. During the course of the year, managers must monitor their budgets and track expenses to ensure that they finish the year within expectations.

Clearly, it's a bad idea to exceed your budget. You might be spending money that doesn't exist, and at the very least, you're going to wind up in hot water with your boss. Privacy managers should keep close tabs on their budgets and make sure that they don't finish the year in the red with a budget shortfall.

The longer you are in business, the more likely it is that you will experience unexpected expenses. You might not be able to predict what unexpected expenses will come up, but it is a fairly safe bet that something you didn't expect will surface. Managers can compensate for this by setting aside a contingency budget designed to cover unexpected expenses.

Although it's definitely a bad idea to exceed your budget, that also doesn't mean that it's a good idea to leave a lot of money on the table. Unless there were very unusual circumstances, a large surplus at the end of the year probably means that you didn't plan very well. You don't run the risk of spending money that isn't there, but you are preventing your company from using those funds elsewhere. In financial terms, you're creating an opportunity cost by holding funds that the organization could use to take advantage of some other opportunity.

You'll need to develop your own patterns for budget monitoring and reporting. For example, you might begin by reviewing your budget and spending on a weekly basis. Over time, as you get comfortable with financial planning, you might back off to a biweekly or monthly schedule.

Communicating about Privacy

Privacy managers find themselves communicating about privacy to others within their organization on a regular basis. This communication includes both broad awareness messages and tailored messages designed to achieve specific privacy objectives.

Creating Awareness

The success of a privacy program depends on the behavior (both actions and inaction) of many different people. Privacy training and awareness programs help ensure that employees and other stakeholders are aware of their privacy responsibilities and that those responsibilities remain top of mind. Privacy managers are responsible for establishing, promoting, and maintaining a privacy training and awareness program to foster an effective privacy culture in their organizations.

Employee Training

Employees within your organization should receive regular *privacy training* to ensure that they understand the risks associated with your uses of personally identifiable information and their role in minimizing those risks. Strong training programs take advantage of a diversity of training techniques, including the use of *computer-based training (CBT)*.

Not every user requires the same level of training. Organizations should use *role-based training* to make sure that individuals receive the appropriate level of training based on their job responsibilities. For example, a systems administrator should receive detailed and highly technical training, whereas a customer service representative requires less technical training with a greater focus on the front-line interactions that they may encounter in their work.

You'll also want to think about the frequency of your training efforts. You'll need to balance the time required to conduct training with the benefit from reminding users of their responsibilities. One approach used by many organizations is to conduct initial training whenever an employee joins the organization or assumes new job responsibilities and then

use annual refresher training to cover the same material and update users on new privacy issues.

The team responsible for providing privacy training should review materials on a regular basis to ensure that the content remains relevant. Changes in the privacy landscape and the organization's business may require updating the material to remain fresh and relevant.

Role-Based Training

All users should receive some degree of privacy education, but organizations should also customize training to meet specific role-based requirements. For example, employees handling credit card information should receive training on Payment Card Industry Data Security Standard (PCI DSS) requirements. Human resources team members should be trained on handling employee information. IT staffers need specialized skills to implement privacy controls. Training should be custom-tailored to an individual's role in the organization.

Ongoing Awareness Efforts

In addition to formal training programs, a privacy program should include *privacy awareness* efforts. These are less formal efforts that are designed to remind employees about the privacy lessons they've already learned. Unlike privacy training, awareness efforts don't require a commitment of time to sit down and learn new material. Instead, they use posters, videos, email messages, and similar techniques to make privacy a top priority for those who've already learned the core lessons.

Building a Communications Plan

Training and awareness efforts should be part of a broader communications plan that privacy professionals develop to inform their communications with various stakeholders over the course of the year. This plan should coordinate all planned communications. In addition to the organization's awareness effort, the plan may include all legally required privacy notices and disclosures. The communications plan provides a single point of tracking and coordinating these messages to ensure that they are timed effectively and are not overlooked.

The communications plan should also ensure that employees have access to current privacy policies and procedures related to their roles and are notified when there are updates to those documents.

While many privacy programs emphasize transparency, companies should also be conscious of the risks of disclosing information. Prematurely sharing information about privacy risks may increase the opportunity for security incidents, create reputational damage, result in regulatory fines, or cause other harm to the organization. Communications plans should consider these risks and involve legal teams and other stakeholders when identifying appropriate timing of communications and levels of detail.

Privacy Program Operational Life Cycle

The privacy program operational life cycle describes the core activities of a privacy program and how the organization addresses each of its major privacy objectives. The four components of the privacy program operational life cycle are:

- **Assess** documents the baseline of the organization's privacy program, evaluates vendors and data processors, and conducts assessments of privacy-related matters. Chapter 3, "Privacy Operational Life Cycle: Assess," focuses on the Assess phase of the life cycle.
- **Protect** includes information security practices designed to safeguard information, the implementation of privacy by design (PbD) principles, the integration of privacy requirements into functional areas of the organization, and technical and organizational measures used to protect data. Chapter 4, "Privacy Operational Life Cycle: Protect," focuses on the Protect phase of the life cycle.
- **Sustain** includes monitoring the privacy program's effectiveness through internal monitoring practices and both internal and external audits. Chapter 5, "Privacy Operational Life Cycle: Sustain," focuses on the Sustain phase of the life cycle.
- **Respond** covers how the organization reacts to data subject information requests and privacy rights and how the organization responds to privacy incidents. Chapter 6, "Privacy Operational Life Cycle: Respond," focuses on the Respond phase of the life cycle.

The major benefit of the life cycle approach to privacy is that it helps maintain the flexibility that is so crucial to the privacy program's success. This life cycle allows the organization to adapt its privacy practices as business needs and regulatory requirements change. It also allows the organization to use the lessons learned from privacy incidents to improve its privacy controls and reduce the likelihood of a future incident.

The focus of privacy programs has shifted over the years. While all four activities of the privacy program life cycle are crucial, early programs often found themselves in a reactive crisis management mode that focused on responding to privacy incidents. Today, most organizations spend much more time and energy in the earlier stages of the life cycle, as they hope to proactively manage risks to prevent incidents from occurring.

Summary

The privacy program serves as the umbrella organizational unit for all of an organization's efforts to protect personally identifiable information. The chief privacy officer (CPO), or other senior privacy leader, bears overall responsibility for ensuring that the privacy program is properly designed, implemented, and operated.

The CPO must ensure that the privacy program remains aligned with the objectives of the business overall as well as the operational objectives of other business functions, including procurement, accounting, human resources, information technology, and audit functions. In addition, the CPO should put monitoring procedures in place to evaluate the effectiveness of the program over time and detect opportunities for improvement.

Exam Essentials

Designate a senior individual accountable for the privacy program. Placing responsibility for the design, implementation, maintenance, and monitoring of a privacy program in the hands of a senior official provides direct accountability for the program's goals and objectives. Organizations commonly designate a chief privacy officer (CPO) to hold these responsibilities, and that CPO may also serve as the organization's point of contact for privacy regulators.

Develop a privacy program designed to achieve the organization's privacy mission. Privacy programs consist of the policies, procedures, tools, and practices used to achieve the desired level of privacy in an organization. Privacy programs should have a high-level strategic purpose/mission that is mapped to more tactical goals and even more specific objectives for achieving those goals. The purpose of a privacy program should change infrequently, whereas goals and objectives may change more frequently.

Describe the purpose of the privacy program. The core of the charter is the scope statement, which defines the privacy objectives included in the program and the portion of the organization covered by the program. The charter should also address the business purpose of the program, a statement of authority, roles and responsibilities, governance structures, documentation, enforcement mechanisms, and processes for periodic program reviews.

Explain how privacy training and awareness ensure that individuals understand their responsibilities. Privacy training programs impart new knowledge to employees and other stakeholders. They should be tailored to meet the specific requirements of an individual's role in the organization. Privacy awareness programs seek to remind users of the information they have already learned, keeping their privacy responsibilities top of mind.

Know that privacy managers are people managers. Privacy managers lead a team of professionals and are responsible for the motivation, development, and management of those team members. This includes providing training that helps employees keep their skills current and certifications that help employees validate their skills.

Know that privacy managers are financial managers. Privacy managers bear responsibility for managing a budget allocated to the privacy program. They must understand how to work within the budgeting and accounting processes used by their organization.

Review Questions

1. Which of the following types of information should be protected by a privacy program?
   - **A.** Customer records
   - **B.** Product plans
   - **C.** Trade secrets
   - **D.** All of the above

2. What data governance model operates by focusing all data governance resources in a single office that serves the entire organization?
   - **A.** Centralized
   - **B.** Distributed
   - **C.** Hybrid
   - **D.** Oppositional

3. Howard is assisting his firm in developing a new privacy program and wants to incorporate a privacy risk assessment process into the program. If Howard wishes to comply with industry best practices, at least how often should the firm conduct these risk assessments?
   - **A.** Monthly
   - **B.** Semi-annually
   - **C.** Annually
   - **D.** Bi-annually

4. Of the following fields, which fits into the "special categories of personal data" under GDPR?
   - **A.** Banking records
   - **B.** Union membership records
   - **C.** Educational records
   - **D.** Employment records

5. Katie is assessing her organization's privacy practices and determines that the organization previously collected customer addresses for the purpose of shipping goods and is now using those addresses to mail promotional materials. If this promotional use was not previously disclosed, what privacy principle is the organization most likely violating?
   - **A.** Quality
   - **B.** Management
   - **C.** Notice
   - **D.** Security

6. Kara is the chief privacy officer of an organization that maintains a database of customer information for marketing purposes. What term best describes the role of Kara's organization with respect to that database?
   - **A.** Data subject
   - **B.** Data custodian
   - **C.** Data controller
   - **D.** Data processor

7. Richard would like to use an industry standard reference for designing his organization's privacy controls. Which one of the following ISO standards is best suited for this purpose?
   - **A.** ISO 27001
   - **B.** ISO 27002
   - **C.** ISO 27701
   - **D.** ISO 27702

8. Which of the following organizations commonly requests a formal audit of a privacy program?
   - **A.** Management
   - **B.** Board of directors
   - **C.** Regulators
   - **D.** All of the above

9. Which element of a privacy program is likely to remain unchanged for long periods of time?
   - **A.** Mission
   - **B.** Goals
   - **C.** Objectives
   - **D.** Procedures

10. Which phase of the privacy program operational model includes the implementation of privacy by design (PbD) principles?
    - **A.** Respond
    - **B.** Sustain
    - **C.** Protect
    - **D.** Assess

11. Which one of the following statements is not correct about privacy best practices?
    - **A.** Organizations should maintain personal information that is accurate, complete, and relevant.
    - **B.** Organizations should inform data subjects of their privacy practices.
    - **C.** Organizations should retain a third-party dispute resolution service for handling privacy complaints.
    - **D.** Organizations should restrict physical and logical access to personal information.

12. Which one of the following is not a common responsibility for an organization's chief privacy officer?

A. Managing privacy risks

B. Encrypting personal information

C. Developing privacy policy

D. Advocating privacy strategies

13. When designing privacy controls, an organization should be informed by the results of what type of analysis?

A. Impact analysis

B. Gap analysis

C. Business analysis

D. Authorization analysis

14. Abe works for an organization that has several subsidiaries that operate independently. Those subsidiaries report to different leaders and have their own independent privacy programs. If the governance model does not change, what would be the appropriate way for Abe's privacy program to address this situation?

A. Limit the objectives of his program.

B. Limit the scope of his program.

C. Include the subsidiaries in his program.

D. Replace the subsidiary programs with his own.

15. Which element of the privacy program operational life cycle includes responding to data subject information requests?

A. Protect

B. Assess

C. Sustain

D. Respond

16. Leo is responsible for managing his organization's privacy budget. Which one of the following circumstances is the most preferred situation?

A. Expenses greatly exceed budget.

B. Expenses slightly exceed budget.

C. Expenses are slightly under budget.

D. Expenses are greatly under budget.

17. Which one of the following elements is *least* likely to be found in a privacy program charter?

A. Scope statement

B. Project schedule

C. Roles and responsibilities

D. Governance structure

18. Tanya is hiring a new incident analyst to help supplement the capabilities of her team. She is identifying the line item in her budget that will cover the salary and benefits for this new employee. What term best describes this expense?

A. One-time

B. Capital

C. Unbudgeted

D. Operational

19. In what Supreme Court case did the term "right to be let alone" first appear?

A. *Olmstead v. United States*

B. *Carpenter v. United States*

C. *Roe v. Wade*

D. *Katz v. United States*

20. Matt wants to share some information gathered from student records but is concerned about disclosing personal information. To protect privacy, he discloses only a table of summary statistics about overall student performance. What technique has he used?

A. Anonymization

B. Deidentification

C. Aggregation

D. Redaction