– Practice Guide

AUDITING PRIVACY RISKS
2ND EDITION

JULY 2012

The Institute of Internal Auditors | Global

Table of Contents

Executive Summary

Why Is Privacy Important?

One of the many challenging and formidable risk management issues faced by organizations today is protecting the privacy of personal information about customers, employees, and business partners. Consumers are concerned with how businesses and organizations use and protect this information. Business owners and management want to meet the needs and expectations of their customers, business partners, and employees; keep any commitments pursuant to contractual agreements; and comply with applicable data privacy and security laws and regulations.

Privacy is a global issue. Many countries have adopted privacy legislation governing the use of personal information, as well as the export of this information across borders. For businesses to operate effectively in this environment, they need to understand and comply with these privacy laws. Examples of influential privacy legislation include Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the European Union's (EU's) Directive on Data Privacy, and privacy acts from Australia, Japan, and New Zealand. Industry-sector privacy legislation from the United States includes the Gramm-Leach-Bliley Act (GLBA) for the financial services industry and the Health Insurance Portability and Accountability Act (HIPAA) for the health care industry.

There are many news stories about security breaches that involve the loss or disclosure of personal information. A greater number of organizations are outsourcing business processes and applications that contain personal information in addition to using new technologies that can increase their privacy risk profile. Stakeholders such as boards[1], audit committees, and other oversight groups want assurance around the organization's processes that protect personal information.

The Benefits of Good Privacy Governance and Controls

Good governance involves identifying significant risks to the organization — such as a potential misuse, leak, or loss of personal information — and ensuring appropriate controls are in place to mitigate these risks. For businesses, the benefits of good privacy controls include:

- Protecting the organization's public image and brand.
- Protecting valuable data on the organization's customers, employees, and business partners.
- Achieving a competitive advantage in the marketplace.
- Complying with applicable privacy laws and regulations.
- Enhancing credibility and promoting confidence and goodwill.

For public-sector and nonprofit organizations, the benefits of good privacy controls also include:

- Maintaining trust with citizens and noncitizens.
- Sustaining relationships with donors of nonprofit organizations by respecting the privacy of their activities.

Sustaining Effective Privacy Practices

Most organizations recognize the need for implementing good privacy practices. However, the challenge is sustaining these practices. With the proliferation of technology that enables the collection, use, disclosure, retention, and destruction of personal information in large volumes and extensive outsourcing of information technology (IT) and business processes in domestic and overseas locations, organizations may have difficulty identifying where this

[1] The term board is used in this guidance as defined in the *International Standards for the Professional Practice of Internal Auditing* (*Standards*) glossary: "a board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report."

data is stored, how it is protected, who has access to it, and whether it is disposed securely. The rapid evolution of technology, such as mobile computing, social networking, radio frequency identification (RFID), and location-based services, has increased the availability of and accessibility to personal information about customers, employees, and others. This evolution has outpaced legal frameworks, as well as industry and individual organization's standards and practices needed to protect the privacy of this valuable asset. In addition, accountability and responsibility for maintaining a privacy program is not always clearly assigned and is often distributed throughout the organization. This can lead to inconsistency and uncertainty when it comes to ensuring good privacy practices are in place and are working effectively.

Introduction

As presented in The IIA's Practice Advisory 2130.A1-2: Evaluating an Organization's Privacy Framework, the internal audit activity can contribute to good governance and risk management by assessing the adequacy of management's identification of risks related to its privacy objectives and the adequacy of the controls established to mitigate those risks to an acceptable level. The following describes some of the benefits of undergoing a privacy audit.

Privacy Audit Benefits

- Facilitates compliance with laws and regulations.
- Measures and helps improve compliance with the organization's data protection system.
- Identifies potential inconsistencies between policies and practices.
- Increases the level of data protection awareness among management and staff.
- Provides information for a data protection system review.
- Provides assurance over reputational risks.
- Improves procedures for responding to privacy complaints.

This practice guide complements and expands on Practice Advisory 2130.A1-2. The guide provides the chief audit executive (CAE) and internal auditors with insight into privacy risks that the organization should address when it collects, uses, retains, discloses, and disposes of personal information. This guide provides an overview of key privacy frameworks to help readers understand the basic concepts and find the right resources for more guidance regarding expectations and what works well in a variety of environments. It also provides direction on how internal auditors can complete privacy assessments.

What is Privacy?

Privacy can take on several meanings and is often discussed in many contexts. It can be seen as descriptive or prescriptive, as a moral interest or a legal right. It can mean freedom from unwanted attention from others or freedom from observation or surveillance. It can cover the privacy of communication as well as information. In its simplest form, *privacy* has been defined as "the right to be let alone."[2]

Privacy definitions in the business environment vary widely depending on country, culture, political environment, and legal framework. In many countries, privacy is closely linked to data protection. Of particular importance to organizations is how privacy is defined in their context. Whether using one of the definitions in Figure 1, or simply defining *privacy* as the protection of the collection, storage, processing, dissemination, and destruction of personal information, the many definitions of privacy can be used by any organization to guide its privacy program.

[2] "The Right to Privacy," Warren and Brandeis, Harvard Law Review, Vol. IV December 15, 1890, No.5.

Figure 1–Privacy Definitions

"Privacy is the protection of personal data and is considered a fundamental human right."
— *Organisation for Economic Co-operation and Development (OECD) Guidelines, 1980*

"Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."
— *European Union (EU) Directive, 1995*

"The rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information."
— *The American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA), 2009*

In today's business context, privacy often refers to the personal information about an individual and the individual's ability to:

- Know how his or her personal information is handled.
- Control the information collected.
- Control what the information is used for.
- Control who has access to the information.
- Amend, change, and delete the information.

Personal information is data that can be linked to or used to identify an individual either directly or indirectly. Some personal information is considered sensitive, as described in Figure 2. Privacy of personal information can be maintained by assuring adequate treatment and protection.

Figure 2–Examples of Personal and Sensitive Information

PERSONAL INFORMATION	• Name. • Gender. • Date of birth. • Home address. • Personal telephone number. • Personal email address. • Government identifier (e.g., identity card, social security number). • Biometric identifier. • Photograph or video identifiable to an individual. • Behavioral information (e.g., in a customer relationship management system).
SENSITIVE HEALTH INFORMATION	• Medical records. • Health plan beneficiary information. • Physical or mental health information. • Provided health services or any information collected during the health service.
SENSITIVE FINANCIAL INFORMATION	• Account numbers (e.g., bank accounts, credit cards). • Financial history. • Salary information.
OTHER SENSITIVE INFORMATION	• Racial or ethnic origin. • Religious or philosophical beliefs. • Political opinions. • Trade union membership. • Legal proceedings and civil actions. • Combinations of certain information.

Some information, although not personal by itself, becomes personal and sensitive when combined with other information. Sensitive personal information generally requires an extra level of protection and a higher duty of care. Implementing a data classification methodology that includes personal information is an effective way for the organization to address the appropriate level of protection and duty of care needed. It provides guidance to help deliver and ensure consistent practices throughout the organization based on the nature of the data.

Privacy Protection

Privacy protection can be considered a process of establishing an appropriate balance between privacy and multiple competing interests. To minimize intrusiveness, maximize fairness, and create legitimate, enforceable expectations of privacy, a set of principles governing the processing of an individual's personal information and a model of the privacy roles involved has evolved over decades (see Figure 3). The principles include a blend of substantive concepts such as data quality, integrity, and limitation of use, and procedural principles such as the concepts of consent and access rights.

Figure 3–Privacy Roles

When implementing a privacy program, there are major roles to consider:

Data subject — Individual whose personal information is collected, used, disclosed, retained, and disposed of.

Data controller — Organization that controls access to and processing of personal information.

Privacy officer — An organization's privacy oversight, monitoring, and contact function.

Privacy commissioner — A governmental oversight authority.

Service providers — Circumstances where third parties are involved in processing personal information.

The way an organization manages personal information about customers, employees, and business partners that it collects, uses, retains, protects, discloses, and disposes of is at the core of the privacy issue for businesses. Recent incidents of identity theft, mismanagement of personal information, and violation of privacy principles have increased regulatory and consumer pressure on organizations to develop appropriate controls in relation to privacy, data management, and information security.

Privacy Risks

Privacy is a risk management issue for businesses, governments, and nonprofit organizations. Surveys continue to show that consumers and citizens are concerned with how organizations use their personal information. Failure of management and data controllers to address the protection of personal information presents numerous risks to the organization, including:

- Possible damage to the organization's public image and branding.

- Potential financial or investor losses.
- Legal liability and industry or regulatory sanctions.
- Charges of deceptive practices.
- Customer, citizen, or employee distrust.
- Loss of customers and revenues.
- Damaged business relationships.

Privacy Controls

Providing adequate governance and oversight by boards and management is an essential control for addressing privacy risks faced by the organization. Other basic privacy control activities include setting objectives, establishing policies and procedures, and implementing monitoring and improvement mechanisms. In addition, the organization should assess privacy compliance and data handling practices and weaknesses, and benchmark them against internal policies, laws and regulations, and best practices.

An effective privacy program includes:

- Privacy governance and accountability.
- Roles and responsibilities.
- Privacy statement/notice.
- Written policies and procedures for the collection, use, disclosure, retention, and disposal of personal information.
- Information security practices.
- Training and education of employees.
- Privacy risk assessments and maturity models.
- Monitoring and auditing.
- Compliance with privacy laws and regulations.
- Inventory of the types and uses of personal information.
- Data classification.
- Plans to address privacy risks for new or changed business processes and system development.
- Controls over outsourced service providers.
- Incident response plans for breach of personal information.
- Plans to address corrective action.

Practice Advisory 2130.A1-2 also recommends that internal auditors contribute to good governance and accountability by playing an assurance and advisory role in helping their organization meet its privacy objectives.

Privacy Frameworks and Principles

3.1 Dealing With Numerous Regulations and Complex Expectations

Many privacy frameworks and principles have been developed and published since the late 1960s. The most useful frameworks are principles-based and usually address the rights of the individual for privacy, but they also try to give weight to the information rights of organizations, businesses, and economies to operate effectively.

Laws and regulations addressing privacy needs are varied, increasingly complex, and rapidly increasing in number by industry, local regulator, nation, or even region. Sound privacy frameworks can help an organization better comply. The core of a useful framework is better articulation of fundamentally accepted privacy principles.

Privacy needs and regulations have been a growing issue. Recognizing the importance of privacy needs, the United Nations formally sponsored studies as early as 1968 and developed principles based on human rights shortly thereafter. More recently, focus has been on developing "generally accepted" privacy principles to help balance conflicts in perspective. For example, governments need to protect individuals from harm, while also protecting society from criminal or terroristic threats by preventive monitoring of information or detective and investigative action using information trails.

Various recent privacy frameworks and principles are useful to those who:

- Oversee and monitor privacy and security programs.
- Implement and manage privacy in an organization.
- Implement and manage security in an organization.
- Oversee and manage risks and compliance in an organization.
- Assess compliance and audit privacy and security programs.
- Regulate privacy.

Figure 4 provides an example of some significant privacy frameworks from laws, regulators, and professional organizations as well as the commonalities of principles among these frameworks.

Figure 4–Privacy Framework Principles[3]

AICPA/CICA GAPP[4]	AUSTRALIA PRIVACY ACT	CANADA PIPEDA	EU DIRECTIVE	JAPAN PERSONAL INFORMATION PROTECTION ACT	OECD GUIDELINES	U.S. FTC[5]
Management.		Accountability.	Notification.	Designate responsibility.	Accountability.	
Notice.	Openness.	Identifying purposes, openness.	Information to be given to the data subject.	Notice, public announcement of purpose of use.	Purpose specification, openness.	Notice.
Choice and consent.	Use and disclosure.	Consent.	Criteria for making data processing legitimate, data subject's right to object.	Consent.	Collection limitation.	Choice.
Collection.	Collection, sensitive information, anonymity.	Limiting collection.	Principles relating to data quality, exemptions, and restrictions.	No unjust method of collecting.	Collection limitation (including consent).	
Use, retention, and disposal.	Identifiers, use, and disclosure.	Limiting use, disclosure, and retention.	Making data processing legitimate; special categories of processing; principles related to data quality, exemptions, and restrictions; the data subject's right to object.	Purpose of use does not exceed its scope.	Use limitation (including disclosure limitation).	

[3] Adapted from the AICPA/CICA's Comparison of International Privacy Concepts.
[4] Generally Accepted Privacy Principles.
[5] Federal Trade Commission.

AICPA/CICA GAPP[4]	AUSTRALIA PRIVACY ACT	CANADA PIPEDA	EU DIRECTIVE	JAPAN PERSONAL INFORMATION PROTECTION ACT	OECD GUIDELINES	U.S. FTC[5]
Access.	Access and correction.	Individual access.	The data subject's right of access to data.	Access and correction.	Individual participation.	
Disclosure to third parties.	Use and disclosure, transborder data flows.	Use and disclosure, transborder data flows.	Transfer of personal data to third countries.	Transfer of personal data, opt-out exception, delegation, merger, joint use.	Use limitation (including disclosure limitation).	
Security for privacy.	Data security.	Safeguards.	Confidentiality and security of processing.	Security control measures.	Security safeguards.	Security.
Quality.	Data quality.	Accuracy.	Principles related to data quality.	Data integrity.	Data quality.	Integrity.
Monitoring and enforcement.	Enforcement by the Office of the Privacy Commissioner.	Challenging compliance.	Judicial remedies, liability and sanctions, codes of conduct, supervisory authority, and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data.	Enforcement.	Individual participation (including challenging compliance).	Enforcement.

3.2 Which Privacy Framework to Use?

It is critical for management to consult its own legal counsel for specific advice on applicable privacy laws and regulations in coordination with how the organization's privacy framework and compliance approach is developed, assessed, and monitored.

The frameworks illustrated in Figure 4 share many common principles. In general, these frameworks are designed to help implement principles articulated by the applicable body. Some are globally, regionally, or nationally applicable, while others cover an industry, regulatory body, or specific set of professional or business needs. From a technical and legal standpoint, frameworks range from binding to fully voluntary, to transnational and national legislation, and to nongovernment organizations. Moreover, they encompass professional standardization bodies such as the International Organization for Standardization (ISO) and industry-driven bodies such as the Payment Card Industry (PCI) Security Standards Council.

No Single-source Solution

Identifying a specific privacy framework that is appropriate for any given organization depends on many factors; as such, it is not addressed in this guidance. In many cases, privacy laws and regulations dictate and influence the privacy framework the organization will adopt. In other situations, individuals and organizations may apply common sense, follow legislation, or pronounce how they plan to respond to potential privacy concerns by group or individual declaration. In any case, it is critical to coordinate and seek advice from legal counsel when developing or adopting a privacy framework.

Privacy — Business, Nonprofits, and Government

Commercial organizations have three major groups of stakeholders: owners/lenders, employees/staff, and customers/general public. Nonprofit organizations have employees/staff and oversight boards to manage their activities. Governmental organizations serve citizens and noncitizens and may have customers as well. In all cases, good governance recommends organizations consider privacy risks, even when they may be based on divergent reasons — from legal rights to just good business practice.

4.1 Privacy Impacts

Organizations use an individual's personal information for various business activities such as market research, customer ratings, rights management, direct marketing, and data trading. This information also may be of interest to the individual's community, friends, family, and professional network.

Personal information also could be collected and used by domestic and foreign governments, competitors, disgruntled employees, hackers, cyberterrorists, saboteurs, and identity thieves. Threats to data subjects require organizations to protect personal information adequately, avoiding adverse consequences and litigation.

4.2 Privacy Threats

Privacy threats and risks may be analyzed using a layered approach that depicts the organization, stakeholder, and individual.

Threats to Organizations

Organizations face tangible threats and risks: They realize the consequences of privacy failures almost immediately. The impact on the organization in the event of a privacy breach often attracts a high level of attention from the press, supervisory authorities, and privacy watchdogs.

Functional threats may restrict an organization's ability to attain its objectives and can cause operational disruption, inefficiency, or ineffectiveness. Threats to an organization's reputation potentially limit its future capability to increase its customer base, serve the needs of clients,

or meet the expectations of citizens. Although privacy threats and risks may limit an organization's capability to perform, a competitive advantage can be gained by managing them effectively. Financial impacts to an organization are of greatest interest to stakeholders; they are mainly a consequence of functional and reputational issues related to privacy risks. Additional privacy risks surface when an organization outsources or cosources some of its business operations, combines or discontinues business activities, or hires, administers, or terminates employees. Other business practices and control weaknesses that potentially elevate the organization's risk profile are listed in Figure 5.

Figure 5–Privacy Control Weaknesses When Processing Personal Data

- Excessive collection.
- Incomplete information.
- Damaged data.
- Outdated information.
- Inadequate access controls.
- Excessive sharing.
- Incorrect processing.
- Inadequate use.
- Undue disclosure.
- Retaining personal information longer than necessary.

Threats to Stakeholders

Although implementing excessive privacy practices and controls may restrict an organization's internal and external processing efficiencies, stakeholders usually face much higher risks from damaged reputation and litigation, thereby reducing the value and profitability of their investment. Maintaining good privacy practices is important in securing the value of shareholders' investments in a corporation.

Threats to Individuals

Individuals often face direct consequences from privacy threats. They may be a victim of identity theft, bear extra cost, experience discrimination, or have limited choices when they offer their personal information to organizations such as governmental agencies, financial institutions, retailers, vendors, and service providers.

For example, when searching for new employment, individuals submit detailed résumés to portals, consultants, or potential employers, who may use their personal information for other purposes without the individual's consent or knowledge. Personal information may be processed through screening and profiling techniques, which may be intrusive, unfair, unreliable, or cause adverse effects for the individual.

4.3 Sector Privacy Issues

It is crucial for internal auditors to understand the legal framework in which the organization operates and take into account all relevant laws, regulations, and other sector guidance. It also is important for the internal auditor to consult with legal counsel when gaining this understanding. This section covers examples of potential privacy issues by sector.

Government and Citizen

A large variety of governmental institutions collect, store, and exchange personal information linked to individuals. Data subjects and data controllers face the constant threat of personal information from vast government files being misused, lost, or stolen.

Public-sector regulation determines how to treat personal information. In many countries, laws exist for the different levels of public entities. Other countries have rules that apply on a case-by-case basis. Therefore, government auditors have to focus on a broad variety of records and programs — for example, real estate records, voter registers, census and opinion polls, taxation records, national

security files, and information collected for welfare programs, social work, education, and law enforcement.

Community Life and Social Services

Many social services institutions — insurers, public welfare programs, and social work programs, as well as other nonprofit organizations — maintain significant and sensitive databases to perform their activities. In many cases, public- or private-sector regulations would apply. Some institutions such as churches may be exempt from general legal frameworks, which may lead to a weak privacy regime. Communities have a high risk of losing the confidence and trust of their constituents when treating personal information without a high regard for confidentiality.

Social security and governmental systems can cause additional exposures through excessive or inappropriate data matching, or comparing personal information from a variety of sources. Often, there are specific rules, laws, and agreements that determine in which circumstances and to what extent data matching and sharing is legitimate. Another problem stemming from data matching is identifiers that could be abused to gather and match data, to manipulate, or to steal an identity.

Financial Services

Financial service organizations such as banks, credit card issuers, funds, and insurers maintain extensive sensitive personal information such as credit ratings, income, spending patterns, place of residence, and credit history. As a result, many regulations and active supervisory bodies exist.

Marketing and Retail

The marketing and retail industry is an extensive collector, user, and distributor of personal information. Personal information maintained for marketing and retail purposes can range from address lists to detailed consumer profiles, financial information, and purchase histories. For example, when an individual makes a purchase, his or her account may be debited immediately, with a record of the transaction showing the date, time, location, and vendor. When you are buying or surfing the Internet, retailers and marketing vendors may use behavioral advertising tracking techniques to monitor and gather personal information. In addition, tracing and tagging mechanisms such as RFID raise privacy issues about the capability to trace individuals.

Personal information is collected from many sources, including point-of-sale, individuals, public sources, information brokers, and other organizations. This information may be used to determine and contact potential customers, define customer clusters using data mining, or create detailed profiles for targeting individual needs and interests.

Sector associations offer various codes of conduct for marketing companies. For example, the Australian Direct Marketing Association (ADMA) provides a self-regulatory code of conduct that covers 10 National Privacy Principles (NPP) to be considered and addressed by all ADMA members.

Communication and Social Media

Communication and social media privacy include the ability to maintain the confidentiality of personal information, as well as the freedom to access media and communication channels. Personal information is captured by customer, subscriber, and lender registers. The entirety of such data can be used to derive preferences and profile individuals. Additional transactional data provides a repository of personal information related to purchase and utilization patterns, including communication partners, time, location, and content. This may cause issues such as spam, eavesdropping, unexpected disclosure of communication and content, and excessive government surveillance.

Utilities, Transportation, and Travel

Utilities and public transportation systems are sophisticated and networked. For example, when an individual passes a toll bridge, a toll is registered through RFID, the license plate is registered with the toll agency, and a credit card is charged. Another system registers the vehicle when it enters a parking lot five minutes later. These integrated systems can generate detailed profiles of individuals by matching data from traffic and access control systems with further transactional information. Many countries foresee the need to establish extra safeguards to avoid the excessive collection of personal data to protect citizen and consumer privacy in these circumstances.

Health Care and Research

Health care providers requires and collects sensitive personal information on patients. Personal information is needed for clinical research, medical services, payment processing, medical testing, and disease management. In the United States, HIPAA protects patients' personal information and applies to health plans, health-care clearinghouses, health-care providers, and employers. The legislation includes key elements such as limiting the use and disclosure of personal information and requiring administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure. Other countries have similar comprehensive laws.

International Businesses

Many laws and regulations require that individuals' personal information not leave the regulated zone. These rules help address the concern regarding loss of control when personal information is transferred to another legal jurisdiction. Organizations that transfer such data could be subject to significant embarrassment, damaged reputations, or financial losses if the information is mismanaged. This creates serious challenges in a world of networked systems, where information is transported across borders within an organization, processed or stored in the cloud — which potentially traverses national boundaries and regulatory jurisdictions — or is shared with trading partners that use and process personal information on a transnational level.

Auditing Privacy

Auditing the organization's privacy practices involves risk assessment, engagement planning and performance, and communication of results. However, there are additional aspects the CAE should take into account, including possible privacy breaches, staff management and record retention issues, and privacy assessments performed by other assurance providers. Many of these aspects are covered by practices of the internal and external audit professions. This chapter outlines some of the key issues and methodologies.

It is important for the auditor to communicate with legal counsel in the early stages of an engagement to discuss the objectives and scope of a privacy audit as well as to determine whether the audit and report of findings should be performed under attorney-client privilege.

5.1 Internal Auditing's Role in the Privacy Framework

An organization's governing body is responsible for deciding the risk it is willing to take and to ensure that resources are in place to manage risk according to that appetite. Addressing privacy risks includes establishing an appropriate privacy framework consisting of policies, procedures, and controls. Internal audit can evaluate that framework, identify significant risks, and make appropriate recommendations to enhance the privacy framework. When evaluating an organization's privacy framework, internal auditors should consider:

- Liaising with legal counsel to understand legal implications:
  - Laws and regulations in all jurisdictions in which business is conducted.

  - Impact of laws and regulations in all jurisdictions in which personal information transverses, is collected, or is stored.
  - Determine whether the privacy assessment should be under attorney-client privilege.

- Liaising with persons responsible for privacy within the organization to understand:
  - Internal privacy policies and guidelines.
  - Privacy policies intended for customers and the public.
  - The maturity of the organization's privacy controls.

- Liaising with IT specialists and business process owners to understand information security implications:
  - Internal security policies and procedures.
  - Security policies communicated to customers and the public.
  - Information flows, system controls, storage, and use of personal information.
  - Incident response programs and plans.

Typical areas that internal audit may review when auditing privacy include:

- Governance/management oversight.
- Privacy policies and controls.
- Applicable privacy notices.
- Types and appropriateness of information collected.
- Systems that process, store, and transmit personal information.
- Collection methodologies.
- Consent and opt-in/opt-out management.
- Uses of personal information for compliance with stated intent, applicable laws, and other regulations.
- Security practices, operations, and technical controls in place to protect personal information.
- Retention and disposal practices of personal information.

For additional considerations, refer to the Appendix, under Privacy Control Weaknesses and Actions Matrix–An Illustration.

Internal auditors should be careful not to assume responsibility for developing and implementing the privacy program, as this may impair their independence. Due to the complex regulatory and technical landscape impacting privacy, legal counsel should be engaged and consideration should be given to procuring third-party expertise for guidance as necessary.

5.2 Engagement Planning

Examples of privacy-related themes that would impact the nature of work by the internal auditor include:

- Ever-changing laws and regulations throughout the world to protect individual privacy.
- Protecting the personal information of individuals in third-party/cloud computing arrangements.
- The maturity level of the organization's privacy practices, policies, and procedures.
- New technologies and business strategies that expose personal information to greater risk.
- Outsourcing and off-shoring of business processes that collect, use, retain, disclose, and dispose of personal information.
- Increased collection, use, disclosure, retention, and disposal of personal information.
- Continued threat of exposure to privacy breaches underscoring the need for a comprehensive privacy incident response plan.

5.3 Prioritizing and Classifying Data

A data inventory and classification program will assist in identifying and prioritizing critical business data, including personal information requiring protection. The auditor should determine the organization's data classification levels, the framework used to classify data, and the baseline controls established for each classification. To assist in this determination, the auditor can ask the following questions:

- Does the organization have a comprehensive data classification policy? Are the levels of classification appropriate to ensure adequate controls? Are the classifications defined adequately?
- Has personal information data been classified? Are the levels of classification appropriate for ensuring adequate privacy controls? Has the data classification policy been communicated to those who are involved — including third-party service providers — in handling the data, from receipt through disposal? Is there a process to monitor changes in laws and regulations that would impact data classification? Are the classifications reviewed periodically to ensure they remain appropriate?
- Has data ownership for personal information been assigned, and have appropriate controls been established in handling the data?
- What are the regulatory penalties for mishandling privacy-protected data? What legal recourse would the impacted individuals have?
- How much harm can be caused to an individual if the information was unintentionally disclosed to unauthorized persons?
- How widely would a privacy breach be disclosed?
- Who would need to be notified? How will they be notified?
- How costly would it be to remedy various types of unauthorized privacy disclosures?
- How would a privacy breach impact customer, citizen (in case of a public entity), or investor confidence? How much would it cost to recover trust and confidence?

5.4 Assessing Risk

Four major areas of risk should be addressed throughout audit planning and when preparing the individual risk assignment: legal and organizational, infrastructure, application, and business process.

Legal and Organizational Risks

Legal and organizational risks include areas such as noncompliance with laws and regulations, lack of governance and privacy leadership, and insufficient resources to maintain an effective privacy program. Some questions to ask when addressing legal and organizational risks as part of the planning for a privacy audit include:

- Who are the designated privacy contacts? What percentage of their time is devoted to privacy issues, and is it adequate?
- Do they have sufficient knowledge, authority, budget, and management support to implement and maintain the privacy program?
- How do the organization's privacy leaders maintain their knowledge of laws and regulations that impact the organization? Have they noted the privacy laws and regulations that impact their business? How do they monitor changes in laws and regulations and evaluate their impacts on the organization's policies, procedures, and systems? How do they work with the data owners to implement appropriate controls to respond to the changes?
- How involved are the organization's privacy contacts in the evaluation of new technologies and business programs to determine their potential privacy impacts?

- If the organization uses cloud computing services, has consideration been given to the privacy implications arising from the geographic location of the data and possible international transfers of personal information governed by international security and privacy laws, and do the contracts address these risks and security requirements adequately?
- Does the organization have a plan to respond to a privacy incident? Are the appropriate people included in the plan? Is the plan documented and up to date? Does it include requirements for breach notification in compliance with all the disparate international, national, and local regulations? Does the breach response plan include steps to lock down involved systems to preserve evidence needed for forensic investigation of the breach?
- Are templates of needed documentation for breach response already prepared, including a notification letter, frequently asked questions for those impacted, instructions for consumers to freeze credit reports, and a basic press release?

Infrastructure Risks

A basic principle of information security is to provide confidentiality, integrity, and availability of data, which coincides with many of the goals of a privacy program. An audit of a privacy program will necessarily involve significant review of information security controls. A challenging area may be identifying how personal information flows in and out of the organization, as well as where and how the information flows among third parties outside the organization.

Information has to enter and leave the application to be useful, often changing media several times during its useful life. The data can start as paper; be transported across the Internet; be processed in the cloud; obtained from, sent to, or stored on mobile devices; stored on a magnetic disk; printed out and put into a filing cabinet; backed up on an optical disk; and later sent off-site to a third party on tape. Each time personal information moves and changes format, new potential vulnerabilities are introduced.

Shredders, encryption, data leakage protection tools, locked files, and many other practices all play a role as countermeasures to leaking sensitive data. Auditors should review the life cycle of personal information the organization obtains from collection to disposal and determine whether it is handled with due diligence along each step.

Specific considerations for the auditor in evaluating the infrastructure risks to privacy include:

- Does the organization have a current data map and inventory of all personal information, including where it resides internally, where it flows into and out of the organization, and how it is transferred among third parties involved in handling personal data on behalf of the organization? Each platform, database, and other technology infrastructure component has its own risks to consider.
- The auditors should trace personal information both in transit over public and private networks and media handled by courier. Auditors also should follow up on stored personal information in production as well as in backup and disaster recovery environments. Specifically:
  - How is personal information encrypted during transmission into and out of the organization and among third parties?
  - Is personal information stored on portable media encrypted?
  - Is personal information encrypted at rest?
- What role do mobile devices play in the collection, handling, and storage of personal information in the organization?
- What general controls are in place on IT platforms where personal information is processed or stored,

including access controls, patch management, and vulnerability scanning?

- Is personal information processed or stored in the cloud? Do cloud service contracts include specifications to ensure the appropriate infrastructure security and controls are in place, and does a right-to-audit clause exist?
- If personal information is being transferred or copied, is the post-transfer residual data treated with the same set of rules as the originating data?

Application Risks

Discovering not only who, but what handles your information becomes critically important when identifying privacy risks. Software can offer speed and accuracy to many error-prone manual functions. Unfortunately, software systems can be complex, with flaws and unintended behaviors. Evaluating software functions is not simple because organizations often mix in-house developed software, customized commercial off-the-shelf software, cloud-based applications and supporting middleware, and operating systems to process, share, and distribute their data.

After the auditor identifies the automated processes, basic security questions need to be addressed regarding any application that handles personal information:

- Was a privacy risk assessment performed to identify and address privacy issues during software development? There is a trend of "privacy by design" that incorporates privacy awareness into every facet of daily business, including the development of new applications and processes involved in personal data collection and use.
- Have data classification standards been implemented in the application to ensure appropriate baseline controls over personal information?
- How was the implementation of the privacy requirements and associated controls validated in development and deployment of the application?
- How does the application authorize and authenticate users? What user roles does the application have to limit access to "minimum necessary" based on their job responsibilities? Are their authorizations reasonable?
- How is user access to personal information tracked and logged to ensure all successful and failed access attempts can be researched and accountability can be established?
- Are there external interfaces to other applications? Do these applications give an equivalent level of control over personal information?
- What is the process for maintaining and upgrading the applications and the underlying database?
- Who responds to potential security issues and ensures that security patches are tested and applied?
- Who is responsible for the general security of the application?
- In development and testing of applications, is test data used or has production data been made appropriately anonymous for personal or sensitive information? If not, are the controls in the test environment equivalent to controls in the production environment?
- Does the application include processing or storing personal information data in the cloud? If so, are the controls equivalent to the controls required for internal applications handling personal information?
- What types of cookies, web beacons, or web pixels are used on the organization's Web applications? Are they for internal use, or are they to gather information for third parties? What type of personal information is collected, how is it used, and, if sensitive, how is the user's consent obtained and stored? Ensuring transparency in the use of these tracking/information-collecting technologies is a key focus of current privacy litigation and regulation.

- Do any applications use geographic location tracking to provide services or obtain personal information from customers? If so, what personal information is collected, how is it used, and, if sensitive, how is the user's consent obtained and stored?

Business Process Risks

Despite technicians' efforts to guard, encrypt, and otherwise secure personal information, the business process will eventually necessitate that personal information is used for its intended purpose. As the personal information is used, it is important that individuals treat it with the level of care corresponding to its data classification. Measures to protect printed personal information should follow the same principles used to classify and protect electronic data. At a minimum, desks should be clean, drawers and filing cabinets should be locked, and record disposal and destruction should be secure. Discretion should be used in areas open to the public. Risk assessments, handling procedures, and training and awareness programs should help to identify and minimize privacy risks inherent in the business processes.

5.5 Preparing the Engagement

Practice Advisory 2130.A1-2 outlines internal audit activities related to an organization's privacy framework. These activities include:

- Assessing the adequacy of management's identification of risks related to its privacy objectives.
- Assessing the adequacy of the controls established to mitigate privacy risks.
- Identifying the types and appropriateness of personal information gathered, the collection methodology used, and whether the organization's use is in accordance with its intended use and applicable legislation.
- Providing assurance on the effectiveness of the organization's privacy policies, practices, and controls.

Approaches to developing a privacy audit program are identified in several regulations and publications. An intuitively sequenced model for an audit program structure, which builds on the OECD criteria, is provided in *Privacy Handbook*[6]. In comparison, *Privacy–Assessing the Risk*[7] presents an exhaustive program with a more technology-oriented structure. Key principles and concepts contained in the AICPA/CICA Generally Accepted Privacy Principles–A Global Privacy Framework along with major international privacy laws and regulations can be very useful in developing privacy themes for the audit program, as shown in Figure 4.

Privacy Assessments

Many legal and regulatory bodies require, or at a minimum, recommend that organizations conduct privacy assessments. Many organizations also realize an operational, internal control, and risk management-driven need to review the effectiveness of privacy policies and practices. Existing assessment models provide extensive guidance for setting up audit work programs. The objectives of a privacy assessment need to be established first. An example of objectives includes:

- To determine inherent and residual privacy-related risks.
- To provide assurance on controls over privacy risks.
- To verify adherence with a set of privacy standards or regulations.
- To ensure compliance with the organization's own privacy statement on the use, collection, retention, protection, and disposal of personal information.

The U.K. Information Commissioner's Data Protection Audit Manual contains a methodology for conducting data protection compliance audits together with a series of checklists aimed at testing compliance with the Data Protection Act of 1998. The audit manual has been tailored to enable any data controller or data owner to help

[6] Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues, Albert J. Marcella Jr. and Carol Stucki, John Wiley & Sons, May 23, 2003

[7] Privacy: Assessing the Risk, Kim Hargraves, Institute of Internal Auditors Research Foundation, 2003

judge his or her organization's own data protection compliance. Similarly, it also may be used by any organization offering such services to data controllers. The Audit Manual describes general privacy audit processes: external and internal audits, adequacy and compliance audits, and vertical (functional) or horizontal (process) audits. Auditors may begin an assessment by scoping the audit areas — the whole organization, a function, a business process, or a category of information. A fully scoped audit is built to cover all privacy principles. A risk-oriented approach focuses on the key risk areas that can be derived by assessing structural, process, and data category dimensions, based on impact and likelihood of events.

Ready-made work programs available from supervisory bodies, industry organizations, and privacy advocates may prescribe mandatory audit work and generally provide a good starting point for customized regular or one-time audit work programs. The CAE or a delegate should review or approve each internal audit work program before a privacy audit begins. Where a privacy commissioner or comparable function is commissioning or performing privacy reviews, internal audit should review both the sufficiency of the audits performed and the effectiveness of the follow-up mechanism in place.

Foundation for a Privacy Audit–Understanding the Data

It is important to realize that compliance with applicable laws and regulations is a foundational issue that should be addressed when performing a comprehensive privacy risk assessment and audit for an organization. When planning a privacy audit, the auditors should:

- Obtain a comprehensive understanding of the personal information collected and stored, its use by the organization, its processing by technology, and the jurisdictions/countries through which the data is processed.
- Interview the individuals responsible for the organization's privacy policy and its enforcement and/or in-house or outside legal experts to gain an understanding of the privacy laws and regulations governing the business and the type of information handled, as well as the known risks, designed controls, and reported incidents.
- Identify the laws and regulations that govern personal information in the jurisdictions where the organization conducts business.
- Determine the regulations and governmental bodies responsible for enforcing privacy rules. Ask the privacy officer or the individual responsible for privacy compliance how such rules are codified in the organization's policies and procedures.
- Identify the customers', employees', and business partners' personal information that the organization collects. If a data inventory of personal information is available, that may provide a starting point for the auditor. If there is no documented inventory, interviews with business process owners and their IT counterparts may be necessary to identify what personal information is collected. Also, automated discovery tools can assist the auditor in this phase.
- Identify what, if any, personal information is shared with third parties. Determine how the data is shared with each of these third parties, including hard copy, file transfer, and portable electronic media. The intent is to identify the formal and informal means by which personal information is shared within the organization and with other entities to identify potential threats, vulnerabilities, and overall risk. Determine whether agreements with third-party service providers and business partners include provisions on appropriate controls for handling personal information from receipt through disposal.

Identify Privacy Threats

Internal auditors should identify privacy threats to the organization through research, benchmarking, and brainstorming, and rank them according to the likelihood of occurrence and impact. Risk assessment meetings with

business process owners also can ensure risks and threats to personal information are explored and identified thoroughly. Assigning values to threats and assets through a privacy risk assessment highlights where the strongest controls or countermeasures should be and the areas on which the auditors should focus to identify vulnerabilities.

A threat uses a vulnerability to exploit an asset. For the purposes of privacy management, the asset is protected personal information. So, who or what is the threat? The threat is the individual or process that, intentionally or not, makes an organization's personal information public or allows any unauthorized access to personal information. A legitimate threat could be a business partner violating contractual obligations or a hacker employed by organized crime. Empirically verified, threats posed by employees, contractors or temporary workers, competitors, developers, janitors, and maintenance staff — those who often have access to stores of confidential information — are very relevant. Whether through malice or carelessness, individuals with access to personal information have the ability to make that information public. If personal information is shared with business partners and contractors, the additional threats to and within their operations and processes should be evaluated.

Identify the Controls and Countermeasures

To determine what the organization is doing to protect personal information from the worst threats, auditors should validate the basic infrastructure and general controls in place, as well as the specific application and internal controls throughout the organization that are active and relied on by the privacy program. Common steps to identify the controls include:

- *Requesting and reviewing documentation*. Review the privacy program as it is implemented in policies, procedures, and other documentation. How do the policies match up with the high-risk areas defined in the privacy risk assessment? How often, if ever, are these policies reviewed? Do they incorporate the latest regulatory and legal guidance? Is the guidance consistent across divisions in the organization? Identify any gaps for follow-up.
- *Interviewing and observing the processing of personal information in action.* The gap between the written policy and the operational action can be significant. Sit with employees on the front lines in operations and IT to determine whether they are aware of the impact of their actions/processes in handling personal information. Determine whether the outright requirements, as well as the spirit or intent of the privacy program, motivate the staff's decisions and actions.
- *Reviewing third-party contracts and contacts.* The depth of the review will depend on how the contractors and the personal information handled by them rank in the threat matrix, but the auditor, at a minimum, should review for language compliant with applicable laws and regulations. If right-to-audit clauses are included, are they exercised with appropriate frequency and depth? Another common technique that auditors can use in reviewing third parties is a security/privacy control survey or questionnaire. This will allow the auditor to obtain information about the controls the third party has in place to protect the organization's personal information and help to identify areas that may require follow-up.

Using a third-party provider's controls wholly, or in conjunction with the organization's own controls, may impact the organization's ability to achieve its control objectives. A lack of controls or weakness in third parties' control design, operation, or effectiveness could lead to such things as loss of personal information confidentiality and privacy. Hence, contracts with third-party providers are a critical element and should contain appropriate provisions for data and application privacy and confidentiality.

By this point, the potential high-impact risks should come into sharper focus, but significant questions will remain

unanswered. It is time to test the controls and countermeasures, hitting the highest impact assets and modeling the highest impact threats.

5.6 Performing the Assessment

The common steps throughout an audit are described in detail in The IIA's International Professional Practices Framework (IPPF). When the auditor understands the organization's privacy objectives, its privacy risks, the types of personal information handled, and the legal framework in which the organization conducts business, an audit program including scope, objectives, and timing of the audit can be developed and approved. The audit team will gather information, perform tests, and analyze and evaluate the test work to prepare the report and recommendations.

Test Work Methodologies

After the risk assessment is completed, traditional test work is focused on general, application, and security controls. Potential testing may include methods beyond the usually applied techniques such as vulnerability assessments and penetration tests, physical control tests, and social engineering tests.

Vulnerability Assessments and Penetration Tests

These methods are often cited as assurance methods for network-accessible applications and infrastructure. Consultants often use terms such as "tiger team" or "ethical hacking" to describe this methodology of identifying and exploiting vulnerable services in a production environment.

Vulnerability assessments generally focus on identifying potential vulnerabilities in information systems. The assessments identify and prioritize vulnerabilities in the configuration, administration, and architecture of information systems. Penetration tests take vulnerability assessments one step further, exploiting the identified vulnerabilities. Penetration tests generally require a higher degree of technical skill and could potentially disrupt production systems. Vulnerability assessments and penetration tests require a set of skills that the internal auditor may need to acquire, either through contracting third-party expertise or training.

Physical Control Tests

Personal information is not limited to digital data. If the organization's modeled threat has access to the building, all the encryption, firewalls, and patched databases in the world cannot keep that individual from retrieving printed information from the trash or accessing data through an unlocked workstation. Digging through trash for protected information, identifying logged-in and unattended workstations, and reviewing secure information storage and handling processes may identify vulnerabilities in the handling of private information. This type of test can answer questions such as:

- Is personal information being disposed of according to policy and procedures?
- Are documents containing personal information stored securely prior to disposal or shredding?
- Are working documents with personal information stored securely?
- Are documents or monitors that display personal information viewable by unauthorized personnel?
- Are workstations locked when unattended?
- Is the application of privacy controls consistent across various departments?

Social Engineering Tests

Social engineering, in the context of security, is the technique of gaining unauthorized access through nontechnical deception. In the scope of testing a privacy program, social engineering can be used to test the effectiveness of controls regarding release of personal information. In other words, can an individual obtain personal information by simply asking for it? The auditor could impersonate executives, network administrators, or other authorized users

to "con" or "sweet talk" passwords or personal information from employees who act as key countermeasures. Social engineering tests can help answer some of the following audit questions:

- How effective are the organization's privacy awareness and training programs?
- Is the balance between customer service and restricting personal information appropriate?
- Is the privacy program supported by the corporate culture?

Organizations have different attitudes toward the conning of employees by internal auditors, so build a threat model and identify vulnerabilities carefully. Discuss the process with the human resources and legal teams to ensure the results will be used to improve privacy practices and not for random firing of tested employees.

5.7 Communicating and Monitoring Results

Many privacy audits are evaluations of compliance programs, and the auditor should consult with legal counsel if potential violations are to be included in audit communications. Consultation and coordination with counsel can reduce the conflict between the auditor's responsibilities to document the results of the engagement with the counsel's legal obligation to defend the organization.

Some of the challenges specific to reporting the results of a privacy audit include:

- Getting all of the participants involved in the scope of the privacy audit. An effective privacy program is practiced by nearly all areas of the organization. Be sure that key participants have input.
- Developing a common, understandable language to describe the risks.
- Ensuring that legal counsel has reviewed the proposed audit plan and draft audit report before issuance to ensure that compliance considerations are addressed appropriately.

The CAE should be aware of IIA Performance Standard 2600: Resolution of Senior Management's Acceptance of Risks in the event that he or she believes that senior management has accepted a level of residual risk that may be unacceptable to the organization related to its privacy program and practices.

5.8 Privacy and Audit Management

The IIA's IPPF reminds auditors to take regulations and risks into account when planning, performing, and reporting assurance and consulting assignments. Many other professional bodies, legislators, and supervisory authorities issue a broad variety of guidance and regulations. The privacy of personal information and how the organization manages this asset should be considered when developing the risk-based audit plan.

The internal audit staff is a key part of the organization's governance structure to address privacy. As such, training programs and policies should be in place to provide internal auditors with the necessary background and knowledge to conduct privacy engagements effectively. There also is a need for due diligence to ensure that auditors act in accordance with relevant laws and policies when using personal information during assurance or consulting engagements. Internal auditors should understand that it may be inappropriate — and in some cases illegal — to access, retrieve, review, manipulate, or use personal information when conducting internal audit engagements. Before initiating an audit, the internal auditors should investigate these issues and request advice from legal counsel, if needed. Finally, internal auditors should consider related privacy regulations, regulatory requirements, and legal considerations when reporting information outside the organization.

Top 12 Privacy Questions CAEs Should Ask

1. Does the organization have a governing body in place to address the acceptable level of privacy risk it will take?

2. What level of privacy risk is management prepared to accept?

3. What privacy laws and regulations currently impact the organization or may likely be required in the near future?

4. What type of personal information does the organization collect, who defines what is personal or private, and are the definitions consistent and appropriate?

5. Does the organization have privacy policies and procedures with respect to collection, use, retention, destruction, and disclosure of personal information?

6. Does the organization have responsibility and accountability assigned for managing a privacy program?

7. Does the organization know where all personal information is stored and who has access?

8. How is personal information protected at various levels — databases, networks, system platforms, application layers, and business process/functional levels?

9. Is any personal information collected by the organization disclosed to or processed by third parties?

10. Do employees receive privacy awareness training and have guidance on their specific responsibilities in handling privacy requirements, issues, and concerns?

11. Does the organization have and provide adequate resources to develop, implement, and maintain an effective privacy program?

12. Does the organization complete a periodic assessment to ensure that privacy policies and procedures are being followed and meet new or current requirements?

Appendix

The IIA's International Professional Practices Framework (IPPF)

Internal audit authoritative guidance is addressed in the IPPF, which comprises mandatory guidance and strongly recommended guidance. The three mandatory elements of the IPPF are the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing* (*Standards*). The three strongly recommended elements of the IPPF are Position Papers, Practice Advisories, and Practice Guides.

Specific privacy-related guidance can be found in the The IIA's Code of Ethics, *Standards*, and Practice Advisories. Relevant portions of this guidance are included below.

IIA Code of Ethics

The section on confidentiality states that internal auditors:

- Shall be prudent in the use and protection of information acquired in the course of their duties.
- Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

IIA Practice Advisories

Although in some cases the following advisories are not specifically related to privacy, they are key practice advisories that the internal auditor should be aware of when assessing an organization's privacy program:

2010-1: Linking the Audit Plan to Risks and Exposures

2010-2: Using the Risk Management Process in Internal Audit Planning

2120-1: Assessing the Adequacy of Risk Management Processes

2120-2: Managing the Risk of the Internal Audit Activity

2130-1: Assessing the Adequacy of Control Processes

2130-A1-2: Evaluating an Organization's Privacy Framework

2200-2: Using a Top-down, Risk-based Approach to Identify the Controls to Be Assessed in an Internal Audit Engagement

2300-1: Use of Personal Information in Conducting Engagements

Privacy Control Weaknesses and Actions Matrix–An Illustration

The following are examples of possible privacy control weaknesses and potential actions by the internal auditor to address those weaknesses. Note that the examples of weaknesses and actions were not intended to be comprehensive and may not apply in your environment.

CONTROL WEAKNESSES	ACTIONS
The organization does not have a privacy policy and related control framework elements.	Discuss with senior management the need for a documented privacy policy and development of an effective privacy program.
The organization is not complying with its privacy policy.	Review the organization's privacy practices to ensure the organization is following the commitments made to customers in its privacy notice.
The organization is not adequately protecting personal information it collects, uses, retains, discloses, and disposes of.	Review the organization's information security practices relating to administrative, physical, and technical controls to ensure personal information is protected adequately.
The organization has not identified the types of personal information it collects, who has access to it, or where it is stored.	Map data flows of personal information collected through automated systems or manual processes, who has access to personal information, and the business need for such access.
The organization has not documented the business purposes for collecting personal information to ensure it does not collect and retain more than necessary.	Map data flows of personal information collected through automated systems or manual processes and identify the business purposes for such collection and retention.
The organization does not have a formal governance structure related to privacy compliance.	Discuss with senior management or the board, if necessary, the need for a governance structure over privacy compliance.
The organization does not have internal privacy policies for protection of personal information.	Review current policies, standards, and procedures related to privacy of personal information to ensure they address areas such as data classification, record management, retention, and destruction.
The organization has not established a compliance auditing or monitoring framework.	Include privacy compliance in the risk-based auditable inventory. Obtain an inventory of laws and regulations that apply to the organization from the legal department. Complete a privacy compliance audit.
The organization does not have an incident response plan in place.	Discuss with senior management — including the IT and legal departments — the need to develop an incident response plan in the event of a breach of personal information.
The organization has not conducted formal privacy awareness, data handling, or information security training.	Review privacy training and awareness materials to determine whether they meet the needs of the organization. Review training records to ensure employees who handle or have access to personal information have undergone the required training.
The organization has not implemented a third-party vendor privacy and security management program to create a consistently applied approach to contracting, assessing, and overseeing the privacy practices of its vendors.	Review contracts of third-party providers to ensure they contain protection requirements for personal information, contract termination clauses, destruction of records containing personal information, and a right-to-audit clause. Perform periodic audits to ensure third-party providers are complying with the contract terms.

Authors:

Ken Askelson, CIA, CPA, CITP, CGMA

Stefanie Hardgrove, CIA, CPA, CIPP/IT

Michael Lynn, CPA

Sara Lademan, CIA, CISA, CGEIT, CISSP

David Williams, CISA, PCI-ISA

Reviewers:

Steve Hunt, CIA, CBM, CGEIT, CISA, CRISC, CRMA

Steven Jameson, CIA, CBA, CCSA, CFE, CFSA, CGMA, CPA, CRMA

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes. For other authoritative guidance materials provided by The IIA, please visit our website at https://globaliia.org/standards-guidance.

Disclaimer

Copyright

The Institute of Internal Auditors | Global

GLOBAL HEADQUARTERS
247 Maitland Ave.
Altamonte Springs, FL 32701 USA

T: +1-407-937-1111
F: +1-407-937-1101
W: www.globaliia.org

120907