

GTAG

GLOBAL TECHNOLOGY AUDIT GUIDE

Managing and Auditing Privacy Risks



The Institute of
Internal Auditors

GTAG Partners



AICPA – American Institute of
Certified Public Accountants
www.aicpa.org



CIS – Center for Internet Security
www.cisecurity.org



CMU/SEI – Carnegie-Mellon University
Software Engineering Institute
www.cmu.edu



ISSA – Information Systems Security Association
www.issa.org



ITPI – IT Process Institute
www.itpi.org



NACD – National Association of
Corporate Directors
www.nacd.org



SANS Institute
www.sans.org

Global Technology Audit Guide 5: Managing and Auditing Privacy Risks

Authors:

Ulrich Hahn, Ph.D., Switzerland/Germany

Ken Askelson, JCPenney, USA

Robert Stiles, Texas Guaranteed (TG), USA

June 2006

Copyright © 2006 by The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means — electronic, mechanical, photocopying, recording, or otherwise — without prior written permission of the publisher.

The IIA publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIA does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

GTAG – Letter From the Chairman

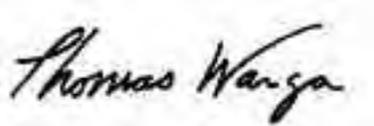
Although today's headlines tend to focus on identity theft and hackers breaking into university and corporate computer files to steal personal information, it is important to remember that the privacy of personal information of employees, customers, and patients is multi-dimensional. As auditors and privacy officers, we need to understand that privacy involves balancing the needs of businesses, government, and consumers. For example, businesses need to gather financial or medical information about customers to reduce the risk of fraud related to lending money or issuing insurance policies. They also need to obtain personal information to comply with anti-money laundering laws. Governments have a responsibility to protect their citizens against acts of terrorism, which may require gathering personal information.

Privacy, from the consumers' and employees' point of view, is about keeping a promise. It's about:

- Gathering the minimal amount of personal information necessary to provide a product or service.
- Protecting personal information against unauthorized view or use.
- Sharing personal information in accordance with the organization's privacy policy.
- Disposing of personal information in a safe manner.

The cost of privacy breaches is increasing everyday. It's not only the financial cost of making it up to a customer who suffered losses due to a privacy breach, but also the cost of reputation damage to the company's brand. Just the other day, I saw a television commercial for a mortgage loan company that said it had the best privacy protection in the industry. With that "promise" to the consumer, the company increased the risk of significant damage to the value of its brand if there ever is a privacy breach.

But, there is good news. *Global Technology Audit Guide 5: Managing and Auditing Privacy Risks* brings the sometimes conflicting dimensions of privacy into sharp focus. It is an excellent guide to help us understand and mitigate privacy risks. I have found this guide to be helpful in clarifying common misconceptions about what privacy risks are and are not. It will help the reader understand the universal principles of privacy, even though specific laws vary by legal jurisdiction. It provides a great framework for assessing privacy risk and provides guidance for the planning and execution phases of a privacy audit.



Thomas J. Warga, CIA
Chairman, The Institute of Internal Auditors (IIA) Inc.

1. Executive Summary for the Chief Audit Executive	1
2. Introduction	3
2.1 What is Privacy?	3
2.2 Privacy Risk Management	4
3. Privacy Principles and Frameworks	6
3.1 Privacy Principles	6
3.2 Privacy Frameworks	7
4. Privacy and Business	10
4.1 Privacy Impacts	10
4.2 Privacy Risk Model	10
4.3 Sector and Industry Issues	11
4.4 Privacy Control Framework	13
4.5 Determining Good and Bad Performers	14
5. Auditing Privacy	17
5.1 Internal Auditing's Role in the Privacy Framework	17
5.2 Activity Planning	17
5.3 Prioritizing and Classifying Data	17
5.4 Assessing Risk	18
5.5 Preparing the Engagement	19
5.6 Performing the Assessment	21
5.7 Communicating and Monitoring Results	22
5.8 Privacy and Audit Management	22
6. Top 10 Privacy Questions CAEs Should Ask	24
7. Appendix	25
7.1 The IIA's Professional Practices Framework	25
7.2 Other Auditing Standards and Methodology	28
7.3 Selected Monographs	29
7.4 Global and Regional Governmental Resources	29
7.5 Regional and National Resources	30
7.6 Professional and Nonprofit Organizations	30
7.7 More Internet Resources	31
7.8 Glossary of Terms	32
7.9 Glossary of Acronyms	36
7.10 Authors, Contributors, and Reviewers	38

Why Is Privacy Important?

One of the many challenging and formidable risk management issues faced by organizations today is protecting the privacy of customers' and employees' personal information. As consumers, we are concerned with how businesses and organizations use and protect this information. As business owners or management, we want to meet the needs and expectations of our customers and employees, keep any promises made to them in the form of privacy policies and notices, and comply with applicable data privacy and security laws and regulations. The organization's customers, suppliers, and business partners want assurances that the personal information collected from them is protected and used only for the purposes for which it was originally collected. When privacy is managed well, organizations earn the trust of their customers, employees, and other data subjects. When it's managed poorly, trust and confidence quickly erode.

"Personal information has become both a significant asset and a liability to its custodians."

— Dr. Ann Cavoukian, *Information and Privacy Commissioner of Ontario, Canada*

Privacy is a global issue. Many countries have adopted nationwide 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. Recent industry sector privacy legislation from the United States includes the Gramm-Leach Bliley Act (GLBA) for the finance industry and the Health Insurance Portability and Accountability Act (HIPAA) for the health care industry.

Article headlines have demonstrated that the privacy and protection of personal information is not absolute. There are many news stories relating to security breaches that involve the loss or disclosure of personal information. More importantly, boards and audit committees want assurance around the organization's processes that protect private information.

The Benefits of Good Privacy 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 and employees.

- 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 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 good practices. With the proliferation of technology that enabled the collection, use, disclosure, retention, and destruction of personal information in large volumes as well as numerous databases, organizations have difficulty identifying where this data is stored, how it is protected, who has access to it, and how it is securely disposed. 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.

To implement and manage an effective privacy program, the organization should clearly define its privacy policies, communicate those policies, and document the procedures and controls relating to the collection, use, retention, and disclosure of personal information to ensure compliance with laws, regulations, and the organization's policies. Specific criteria that are relevant, objective, complete, and measurable should be established for evaluating each of these elements' effectiveness. Establishing these criteria can provide a consistent approach to protecting personal information in a way that individuals can understand easily and the organization can implement and evaluate readily. Established frameworks like the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines as well as recent legislation and professional guidance provide sound and tested criteria against which to benchmark.

The Internal Auditor's Role in Privacy Protection

As presented in The IIA's Electronic Systems Assurance and Control (eSAC) modules and practice advisories on privacy, the privacy and protection of personal information provides a compelling platform for auditors to be active participants in helping their organization address privacy concerns and risks. A key role for internal auditors is to provide an independent assessment of the organization's privacy controls. "Figure 1.1 – Privacy Audit Benefits" describes some of the benefits of undergoing a privacy audit.

The IIA's Practice Advisory (PA) 2100-8: Internal

Figure 1.1 – Privacy Audit Benefits

- Facilitates compliance with the law.
- Measures and helps improve compliance with the organization's data protection system.
- Increases the level of data protection awareness among management and staff.
- Provides information for a data protection system review.
- Improves customer satisfaction by reducing the likelihood of errors leading to a complaint.

Auditing's Role in Evaluating an Organization's Privacy Framework (see the Appendix, page 27) states that the internal auditor can contribute to ensuring good governance and accountability by playing a role in helping an organization meet its privacy objectives. The internal auditor is positioned to evaluate the organization's privacy framework and to identify the significant risks along with the appropriate recommendations for their mitigation.

Scope of GTAG 5

This Global Technology Audit Guide (GTAG) is intended to provide the chief audit executive (CAE), internal auditors, and management with insight into privacy risks that the organization should address when it collects, uses, retains, or discloses personal information. This guide provides an overview of key privacy frameworks to help readers understand the basic concepts and find the right sources for more guidance regarding expectations and what works well in a variety of environments. It also covers how internal auditors complete privacy assessments.

2.1 What is Privacy?

Privacy can take on several meanings and is often discussed in many contexts (see “Figure 2.1 – Privacy Spheres”). Privacy has long been regarded as a basic human right in most societies. 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 be freedom from intrusion or a state of seclusion. 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” (Warren/Brandeis, 1890).

Figure 2.1 – Privacy Spheres

- Personal privacy – Physical and psychological privacy.
- Privacy of space – Freedom from surveillance.
- Privacy of communication – Freedom from monitoring and interception.
- Privacy of information – Control over the collection, use, and disclosure of personal information by others.

— Source: *Canadian Institute of Chartered Accountants (CICA), 2002*

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 2.2 – Privacy Definitions,” or simply defining *privacy* as the protection of the collection, storage, processing, dissemination, and destruction of personal information, the many definitions of privacy are complimentary and can be used by any organization to guide its privacy program.

Figure 2.2 – Privacy Definitions

“Privacy is the protection of personal data and is considered a fundamental human right.”

— *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.”

— *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 (AICPA)/CICA, 2005*

In today’s business context, privacy often refers to the privacy of 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.

Information privacy, which combines communications and data privacy, generally can be described by the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information about an identifiable individual that includes any factual or subjective information, recorded or not, in any form. In other words, information privacy can be maintained by assuring adequate treatment and protection of personal information.

Personal Information

Personal information is data that can be linked to or used to identify an individual either directly or indirectly. Some examples of personal information are:

- Name.
- Home or e-mail address.
- Identifiers such as Social Security, social insurance, passport, or account numbers.
- Physical characteristics.
- Credit records.
- Consumer purchase history.
- Employee files.

Sensitive Information

Some personal information is considered sensitive information. Examples of sensitive personal information include:

- Medical records.
- Financial information.
- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Information related to offenses or criminal convictions.

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.

Anonymized Information

Anonymized information about people cannot be associated with specific individuals. Such information is referred to as *nonpersonal information*. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. When an individual’s identity cannot be determined from the

information that remains, it is considered to be “de-identified” or “anonymized.”

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 past decades (see “Figure 2.3 – Privacy Roles”). The principles include a blend of substantive concepts such as data quality, integrity, and limitation of use, to procedural principles like the concepts of consent and access rights.

Figure 2.3 – Privacy Roles

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

- **Data subject** – Individual whose personal data is controlled.
- **Data controller** – Organization or entity controlling the personal data.
- **Privacy officer** – An organization's privacy oversight and contact function.
- **Privacy commissioner** – The governmental oversight authority, usually on the federal or state level.
- **Service providers** – In circumstances where third parties are involved in data processing.

The way an organization manages the personal information about customers and employees that it collects, uses, distributes, stores, and protects 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. Organizations that fail to address privacy issues adequately run the risk of long-term damage to their brand and reputation, loss of consumer and employee trust, enforcement actions and fines, and criminal prosecution.

Adequate controls can minimize or avoid risks for all parties involved. Internal auditing can play an important role in identifying risks, evaluating controls, and improving an organization's practices regarding privacy of employees, customers, and citizens.

2.2 Privacy Risk Management

Privacy is a risk management issue for businesses and non-profit organizations. Surveys continue to show that consumers are concerned with how businesses use their personal information. Failure of management to address the protection of personal

information properly presents a number of risks to the organization, including:

- Possible damage to the organization's public image and branding.
- Potential financial or investor losses.
- Legal liability or industry or regulatory sanctions.
- Charges of deceptive practices.
- Customer, citizen, or employee distrust.
- Loss of customers or revenues.
- Damaged business relationships.

Privacy Controls

Providing adequate governance and oversight by directors and management (i.e., tone at the top) is an essential control for addressing privacy risks faced by the organization. The CAE should encourage executive management to address how the organization manages, controls, and protects personal information it collects about customers and employees with the audit committee. 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.

It is critical that the organization implements an effective privacy program that includes:

- Privacy governance and accountability.
- A privacy statement.
- Written policies and procedures.
- Controls and processes.
- Roles and responsibilities.
- Training and education of employees.
- Monitoring and auditing.
- Information security practices.
- Incident response plans.
- Privacy laws and regulations.
- Plans for responding to detected problems and corrective action.

The IIA's PA 2100-8: Internal Auditing's Role in Evaluating an Organization's Privacy Framework, suggests that internal auditors can contribute to good governance and accountability by playing a role in helping an organization meet its privacy objectives. Specific activities internal auditors could perform in this area include:

- Working with legal counsel to determine what privacy legislation and regulations would be applicable to the organization.
- Working with information technology management and business process owners to assess whether information security and data protection controls are in place and are reviewed regularly.
- Conducting privacy risk assessments, or reviewing the effectiveness of privacy policies, practices, and controls across the organization.
- Identifying the types of personal information collected, the collection methodology used, and whether the organization's use of the information is

- in accordance with its intended use.
- Reviewing policies, procedures, and guidelines governing data flows and handling procedures designed to safeguard the privacy of personal information, with a focus on identifying potential opportunities to standardize data protection practices across the organization.
- Conducting an assessment of service providers’ interactions, including a review of procedures and controls over providers who manage personally identifiable information or sensitive data on behalf of the organization.
- Reviewing current training practices and materials, and inventorying the privacy awareness and training materials available and needed.

- Performing a gap analysis of data flows and handling procedures against relevant policies, laws, regulations, and best practices for consistency and compliance. This covers assessments of both automated and manual processes for handling personal information that identifies individuals.

Key Privacy Risks and Actions

Internal auditors are positioned to evaluate the privacy framework in their organization and identify the significant risks along with appropriate recommendations for their mitigation. Examples of key privacy risks that internal auditors should address can be found in “Figure 2.4 – Privacy Risk and Actions Matrix.”

Figure 2.4 – Privacy Risk and Actions Matrix

Privacy Risk	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.	Conduct a review of 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, and discloses.	Conduct a review of 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 system data flows of personal information collected, who has access to personal information, and the business need for such access.
The organization does not have a formal governance structure related to privacy compliance.	Discuss with senior management or the audit committee, if necessary, the need for a governance structure over privacy compliance.
The organization does not have internal privacy policies that enhance protection of personal information.	Review current policies, standards, and procedures relating to privacy of personal information to ensure they address such areas 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 information technology 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 material to determine whether it meets 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 key elements of a contract that include 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 terms of the contract.

GTAG – Privacy Principles and Frameworks – 3

The wish for privacy stems from diverging needs, depending on the time, place, situation, and interest of an individual or an organization. A paradigm shift occurred with the spreading of computerized data processing and global communication networks: citizens and consumers became almost fully transparent, leading to exciting opportunities and astonishing experiences, but also threatening the foundations of society and business.

Today's organizations have the benefit of several decades of experience with privacy concepts in a computerized and networked world. Internal auditors play a role in assuring that adequate controls are in place, that controls function reliably, but also that organizations use information efficiently and effectively to achieve their objectives.

Many frameworks have been developed. Some are mandatory and others provide discretionary guidance for the processing of personal information. This section will look at the major frameworks available.

3.1 Privacy Principles

The focus of privacy principles varies: transnational regimes have either a more human rights perspective, as presented by the United Nations (UN) and the Council of Europe (CoE), or a more free trade-oriented rationale, as presented by the OECD and the Asian-Pacific Economic Cooperation

(APEC). National omnibus law usually aims at balancing government-citizen relationships as well as business-consumer relationships.

Privacy issues became apparent with the advent of computerization. The UN's General Assembly picked up on the topic in 1968, commissioning research to understand privacy threats and potential countermeasures. Such global awareness was followed by the first comprehensive federal privacy laws in Sweden in 1973. Germany followed suit a year later, and France established privacy laws in 1978.

In 1980, the OECD member states agreed on fair information practices and placed restrictions on the collection, use, and disclosure of personal information. These practices include:

- Limiting the collection and use of personal information for the purposes intended.
- Ensuring data quality and accuracy.
- Establishing security safeguards.
- Being open and transparent about the practices and policies regarding personal data.
- Allowing individuals access to their personal data and the ability to have it corrected.
- Identifying persons to be accountable for adherence to these principles.

Figure 3.1 – PIPEDA Principles

1. **Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at, or before, the time the information is collected.
3. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as necessary for the fulfillment of those purposes.
6. **Accuracy:** Personal information shall be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used.
7. **Safeguards:** Personal information shall be protected by security safeguards that are appropriate to the sensitivity of the information.
8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

The OECD privacy principles are Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.

The 1996 Canadian Standards Association Model Code for the Protection of Personal Information, now incorporated into national law (PIPEDA), provides a comprehensive consolidation of privacy principles (refer to “Figure 3.1 – PIPEDA Principles” on the previous page).

The 1984/1998 UK Data Protection Act’s principles likewise state personal data should be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant, and not excessive.
- Accurate.
- Not kept for longer than necessary.
- Processed in line with the data subject’s rights.
- Secure.
- Not transferred to jurisdictions without adequate protection.

Such privacy principles are considered essential for the proper protection and management of personal information. They provide guidance for internal auditors charged with reviewing privacy practices.

3.2 Privacy Frameworks

A broad variety of privacy frameworks have emerged since 1968, when the UN recognized that electronic privacy would become a global issue. From a technical and legal standpoint, such frameworks range from binding and voluntarily applicable, to regimes. Some are globally applicable, and others are individual norms. Moreover, individuals and organizations may apply plain common sense, follow legislation, or pronounce how they plan to respond to potential privacy concerns by group or individual declaration (see “Figure 3.2 – Privacy Norms”).

Figure 3.2 – Privacy Norms	
Typology	Scope
• Common sense, ethics.	• Global.
• Constitutional.	• Regional.
• Legislative.	• National omnibus.
• Rules and regulations.	• Sector, industry.
• Soft law, self regulation.	• Individual.
• Seals, certificates.	• Frameworks - on all levels.
• Application of frameworks.	
• Commitment to perform.	

What are the implications for internal auditing and management of audited organizations? Auditors need to know and understand the applicable frameworks and whether the organization is subject to — or expected to follow — any specific framework when providing assurance on privacy controls and risks. The remaining sections of this chapter provide an overview of key frameworks that outline basic privacy concepts as well as information on appropriate resources for more guidance, more detail on expectations, and what works well in a broad variety of places and situations.

Nonbinding Transnational Frameworks

Nonbinding transnational frameworks initially were set up to ensure the free flow of information among organizations’ affiliate countries. The OECD Council’s Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data was created in 1980 to establish a common ground for free transborder data flow among the 24 OECD members. Although not legally binding, the technology-neutral and broadly applicable set of principles became widely accepted over time. OECD committees regularly issue research reports in the area of privacy and data protection.

In 1990, 10 years after the OECD guideline was published, the UN General Assembly issued its human rights-based Guidelines Concerning Computerized Personal Data Files, which member states should take into account when implementing national data protection legislation. The guidelines recommend that member states provide basic information privacy guarantees to their citizens and a set of minimum safeguards for processing personal data comparable to the OECD principles. They also ask for supervisory authorities and address personal data processed by international institutions.

In 2004, the APEC Privacy Framework was developed and is consistent with the core values of the OECD guidelines. It is intended to provide guidance and direction to businesses in APEC economies on common privacy issues and the impact these issues have on the way businesses are conducted.

Legally Binding Transnational Frameworks

Some regional regimes, namely the CoE Convention 108 and the EU Directive 95/46/EC, are binding legal instruments. The CoE Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, published Jan. 28, 1981, binds over 30 signatories to implement the convention’s privacy principles into their national law. Individuals can then appeal to a CoE court in the event that their rights are not sufficiently protected on a national level. The convention’s privacy principles are comparable to the 1980 OECD guideline, with additional safeguards required for sensitive data.

The EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, published Oct. 24, 1995, aims at homogenizing the national regimes of the EU member states to simplify data transfers and strengthen

GTAG – Privacy Principles and Frameworks – 3

individuals' rights. It contains broader and more detailed privacy principles than the OECD guideline as well as additional provisions on sensitive data, disclosure, registration, and opt-out and redress rights. It grants independent supervisory bodies with investigative authority, intervention powers, and the ability to engage in legal proceedings. A later directive regulates the processing of personal data in telecommunications.

National Legislation

National legislation occurs in the form of omnibus laws and sector regulation. Omnibus laws are generally either public- or private-sector laws, as citizens' safeguards against intrusive government action tend to be stronger than legalistic interventions to balance private interest. A detailed review of national legislation is not covered in this GTAG; however, overviews and links can be found at several privacy commissioners' and global privacy initiatives' Web sites (refer to pages 30-32 of the Appendix).

The patchwork of national laws (see "Figure 3.3 – Data Protection Laws") has significant implications for internal auditors. They must understand which laws apply and be able to benchmark existing practices against all legal frameworks that do or could apply. In many cases — for example, when providing services over the Internet — limitation to a specific framework will not be possible. In those situations, internal auditors should consult with internal legal counsel to develop a control-oriented understanding of the general practices,

frameworks, and expectations to evaluate practices and advise management adequately.

Nongovernmental Frameworks

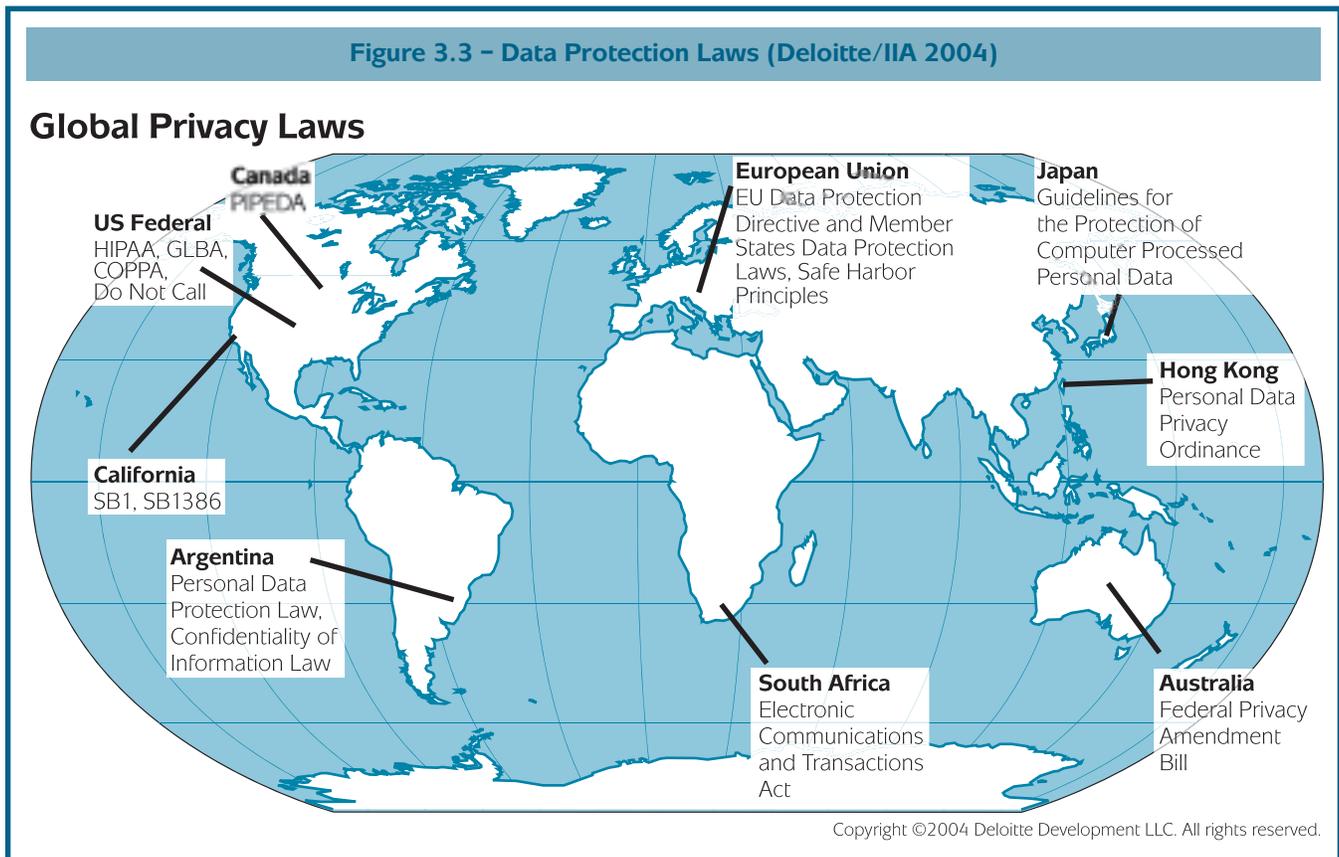
A broad variety of frameworks originate from professional associations, service providers, vendors, standardization bodies, and other interest groups. Some privacy laws — such as those in Australia — foresee that oversight bodies endorse self-regulating privacy codes that may become legally binding after review and publication. Laws may also suggest privacy audits and seals for systems or services, like the German Federal Privacy Law 2003.

Standardization Bodies

The International Standardization Organization (ISO), the American National Standards Institute (ANSI), Canada's Standards Association, Standards Australia, and many other bodies have developed privacy frameworks. Canada's Standards Association's Model Code for the Protection of Personal Information (Q830) sets out 10 principles that balance the privacy rights of individuals and the information requirements of private organizations. Key elements of the privacy code have been incorporated into the Canadian PIPEDA.

ANSI X9.99:2004 (Privacy Impact Assessment Standard for the financial services industry) aims at supporting the implementation of the US GLBA of 1999. The standard recognizes that a privacy impact assessment (PIA) is an important

Figure 3.3 – Data Protection Laws (Deloitte/IIA 2004)



management tool that should be used within an organization or by third parties to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems. The PIA standard describes the privacy impact assessment activity, defines the common components of a PIA, and explains how to improve the quality of business systems based on PIAs.

Standards Australia has developed AS 2805.9-2000: Electronic Funds Transfer – Requirements for Interfaces – Privacy of Communications, which specifies methods of protecting from disclosure the information contained in certain electronic messages. Standards Australia also developed AS 4721-2000: Personal Privacy Practices for the Electronic Tolling Industry, which describes methods of operation and modes of business conduct that should be adopted by operators of electronic toll collection systems and electronic parking station management systems to protect the personal privacy of their customers.

The Platform for Privacy Preferences Project (P3P) is a technical standardization project by the World Wide Web Consortium (W3C) that provides a standard for declaring and negotiating privacy policies between Web site operators and Web users. The standard provides a simple, automated way for users to gain more control over the use of personal information on the Web sites they visit.

Professional Frameworks

The AICPA/CICA developed a comprehensive privacy framework that includes a set of Generally Accepted Privacy Principles (GAPP), which aim to assist organizations with their privacy programs. The GAPP framework was developed from a business perspective, and references significant domestic and international privacy regulations. Each of its 10 principles is supported by objective, measurable criteria that need to be met. The principles are management, notice, choice and consent, collection, use and retention, access, disclosure, security, quality, and monitoring and enforcement.

The GAAP are useful to those who oversee and monitor privacy programs and implement and manage privacy or security. They also can be used for benchmarking, policy design and implementation, and performance measurement. The GAPP framework is a great resource for internal auditors charged with assessing compliance or auditing privacy or security programs (refer to the Appendix, page 28, for the AICPA/CICA GAPP.)

International Federation of Accountants (IFAC) standards relating to privacy engagements are covered by the International Standards on Assurance Engagements (ISAE) 3000. The ISAE establishes basic principles and essential procedures for professional accountants in public practice for the performance of assurance engagements other than audits or reviews of historical financial statements. The ISAE 3000 covers such areas as ethical requirements, quality control, engagement acceptance and continuance, planning and performing the engagement, obtaining evidence, and preparing the assurance report.

Business Frameworks

International Security Trust and Privacy Alliance (ISTPA) is an example of a global alliance of business and technology providers whose goal is to provide objective research and evaluation of privacy standards, tools, and technologies, and to define a privacy framework for building technology solutions. The ISTPA Privacy Framework can be used as a guideline for developing operational solutions to privacy issues and as an analytical tool for assessing the completeness of proposed solutions.

Marketing associations like the Australian Direct Marketing Association (ADMA), the U.S. Direct Marketing Association (DMA), and comparable bodies in other regions have developed self-regulation to guide their members and increase acceptance of their business by individuals as well as consumer rights' advocates.

Privacy Seals

Many organizations conducting business online use privacy seals to gain customer trust and confidence. A privacy seal is an identifiable symbol awarded to a Web operator by a third-party enforcement program to signify that the Web operator has implemented, and is abiding by, effective privacy practices.

According to the Online Privacy Alliance (OPA) organization, characteristics of a privacy seal program offered by a seal provider should include: ubiquitous adoption; comprehensiveness enough to address sensitive and nonsensitive information; accessibility to the user; and affordability. The provider should also be able to pursue avenues to maintain the integrity of the seal, and the provider should have the depth to handle inquiries and complaints.

Some well-known organizations that provide a privacy seal include TRUSTe, BBBOnline, and Webtrust. TRUSTe provides a Web privacy seal to organizations that complete a privacy self-assessment, participate in a Web site audit, and agree to ongoing monitoring and dispute resolution. The BBBOnline Privacy Program awards a privacy seal to businesses that meet program requirements such as:

- Posting an online privacy notice that includes a commitment to privacy and data security and explains how the information is collected and used, how to access or correct information, and how to contact the organization.
- Completing a comprehensive privacy assessment.
- Undergoing monitoring and review by the BBBOnline organization.
- Participating in the program's consumer dispute resolution system.

WebTrust is an AICPA/CICA seal that requires a certified public accountant (CPA) or chartered accountant (CA) audit. It incorporates principles and related criteria with regard to security, availability, processing integrity, privacy, and confidentiality. Each of these principles and criteria are organized in four areas: policies, communications, procedures, and monitoring.

This chapter reviews the impact of privacy issues, threats, risks, and basic control mechanisms needed for mitigation in commercial, nonprofit, and governmental organizations.

Commercial organizations have three major groups of stakeholders: owners/lenders, employees/staff, and customers/general public. Nonprofit organizations have oversight mechanisms in place to manage their fundraising activities, rather than having the owners assume this responsibility. 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 quite divergent reasons — from constitutional rights to just good business practice.

4.1 Privacy Impacts

An individual's personal information is used by organizations for various business activities like market research, customer ratings, rights management, direct marketing, and data trading. It may also be of interest for the individual's community, friends, family, and professional network.

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

4.2 Privacy Risk Model

Privacy risks result from the collection, use, retention, and disclosure of individuals' personal information in their consumer, customer, partner, client, worker, patient, beneficiary, affiliate, or citizen roles. Although it is important to understand the resulting threats to individuals, management and internal auditors will focus assessment primarily on the potential threats to the organization vis-à-vis government, stakeholders, managers, staff, or service providers.

Privacy threats and risks can be analyzed using a layered model that depicts the organization, stakeholder, individual, and society (as displayed in "Figure 4.1 – Categorizing Privacy

Threat, Risk, and Impact"). Privacy failures will have consequences with regard to business function, reputation, finance, and individual.

Threats to Organizations

Organizations face the most tangible threat and risk: they realize the consequences of privacy failures almost immediately. The impact on the organizational level often attains a high-level of attendance from the press, supervisory authorities, and privacy watchdogs.

Functional threats restrict an organization's ability to attain its objectives, cause operational disruption, inefficiency, or ineffectiveness. Threats to an organization's reputation limit its future capability to perform by decreasing the responsiveness of customers, clients, or citizens. Although privacy threats and risks limit an organization's capability to perform, a competitive advantage can be gained by managing privacy threats and risks effectively. Financial impacts to an organization are of greatest interest to stakeholders; they are mainly a consequence of functional and reputational issues relating to privacy risks. Impacts on society result from insufficient performance, financial losses, and adverse effects on society's members. Additional privacy risks surface when an organization outsources or co-sources some of its business operations, combines or discontinues business activities, or hires, administers, or detaches employees.

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. Adequate privacy practices are important to secure the value of stakeholders' investments in a corporation.

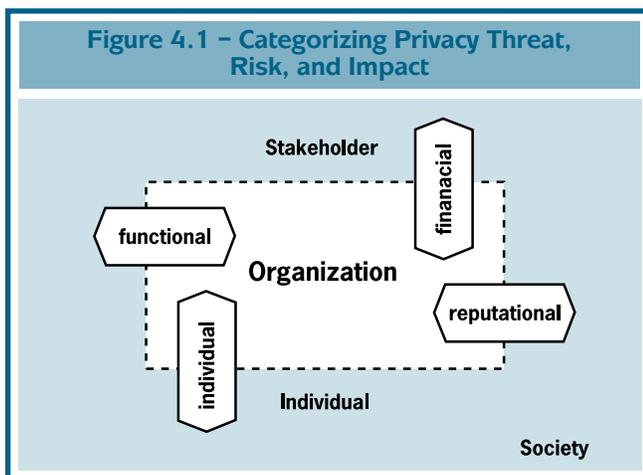
Threats to Individuals

Individuals often face direct consequences from privacy threats. They may bear extra cost, experience discrimination, or have limited choices unless they put their private sphere under excessive risk by offering their data to vendors and service providers.

When searching for new employment, individuals submit detailed resumes 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 to the individual.

Employer monitoring of phone, mail, computers, and office space are a common practice. Individuals rely on the confidentiality of their communication and space when not informed about monitoring practices.

An individual does not have much power to challenge businesses' or governments' privacy practices or get



compensation for damages. This imbalance is the main cause for privacy regulation to protect individuals.

Figure 4.2 – Privacy Risks When Processing Personal Data

- Excessive collection.
- Incomplete information.
- Damaged data.
- Outdated information.
- Inadequate access controls.
- Excessive sharing.
- Incorrect processing.
- Inadequate use.
- Undue disclosure.

Threats to Society

Economic and social development requires a relatively high degree of individual freedom. Whole societies can be manipulated into making undesirable moves if the power of citizens and government are not balanced adequately. Behavioral scientists have observed that citizens can only exert their power effectively if they can keep a minimum private sphere and are able to communicate freely within their community. Hence, the biggest threat to society would be control over individual citizens, defeating societal progress, adaptation, and stabilization mechanisms (see Figure 4.3 – Privacy Threats and Opportunities below).

4.3 Sector and Industry Issues

It is crucial for auditors to understand the legal framework in which the organization operates and take all relevant laws, regulations, and other sector guidance into account. It is also important for the internal auditor to consult with internal legal counsel when providing assessment or consulting activities relating the organization’s privacy program and practices

for the collection, use, disclosure, and retention of personal information. These assessments and consulting services may include:

- Looking for privacy risk drivers, including identification of personal information collected, consequences specific to the organization, and a privacy framework to apply.
- Identifying practices or frameworks of comparable public- or private-sector activities that could be applied.
- Tracking down system interfaces that process personal information and evaluating the basis and effectiveness of any exchange as well as potential exposures to the data subject and the organization.
- In consultation with internal legal counsel, determining if collection and sharing of personal information is excessive and beyond the limits of the processing purpose.
- In consultation with internal legal counsel, evaluating the privacy exposures caused by transnational data transfer and determining specific threats, the risk to the organization, and whether adequate controls are in place.

Government and Citizen

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

Special public-sector regulation determines how to treat personal information. In many countries, umbrella 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 registers and programs — for example, real estate registers, voter registers, census and opinion polls, taxation records, national security files, and information collected for welfare programs and social work, education, and law enforcement.

Figure 4.3 – Privacy Threats and Opportunities

	Threats	Opportunities
Organizations	<ul style="list-style-type: none"> • Litigation. • Negative publicity. • Financial losses, extra cost. • Operational disruptions. • Market failure. 	<ul style="list-style-type: none"> • Market intelligence. • Cost reduction. • Effective communication. • Competitive advantage.
Individuals	<ul style="list-style-type: none"> • Externalized cost. • Surveillance. • Identity theft. • Spam. • Civil rights constraints. 	<ul style="list-style-type: none"> • Personalized services. • Cheaper products. • Targeted offers. • Network building.

Community Life and Social Security

Many social security institutions — insurers, public welfare programs, social work programs, as well as other non-profit organizations — maintain significant and sensitive databases to perform their activities. In many cases, public or private sector umbrella regulations would apply. Some institutions — churches, for example — may be exempt from the general legal frameworks, which may lead to a weak privacy regime. Sensitive data is stored and processed in many cases. Communities have a high risk of losing the confidence and trust of their members when treating personal data inappropriately.

Social security and governmental systems can cause additional exposures through excessive or inappropriate data matching, or comparing personal data 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 and data leaks is identifiers (IDs) 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 including credit ratings, income, spending patterns, place of residence, and credit history. As a result, many regulations and/or active supervisory bodies exist.

Marketing and Retail

The marketing and retail industry is an extensive collector, user, and distributor of personal information. The data 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. The retailer's stock management system electronically captures and retains the article, size, color, and customer IDs. In addition, tracing and tagging mechanisms such as radio frequency identification technologies are starting to appear, raising priva-

cy issues about the capability to trace individuals.

Data is collected constantly from many sources and includes transactional data, data shared with other organizations, data gathered from individuals or public sources, and data bought from information brokers. The information may be used to determine and contact potential customers, to define customer clusters using data mining, or to create detailed profiles for targeting individual needs and interests.

Sector associations offer various codes of conduct for marketing companies. For example, the ADMA provides a self-regulatory Code of Conduct that covers privacy principles to be considered and addressed by all ADMA members (refer to “Figure 4.4 – Direct Marketing Code of Conduct”).

Communication and Media

Communication and media privacy include the ability to maintain the confidentiality of personal information, as well as the freedom to access media and communication channels. Beyond that, 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

The use of utilities was once simplistic and anonymous; a coin dropped into an electricity meter or a toll station, or a paper slip was punched when someone wanted to ride the bus. However, today's systems are sophisticated and networked. When an individual passes a toll bridge, his or her license plate is registered and 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 for establishing extra safeguards or refer to constitutional provisions to avoid the excessive collection of personal data to protect citizen and consumer privacy in these circumstances.

Health Care and Research

Health care requires and produces sensitive information on patients. Personal information is needed for clinical research, medical services, medical testing, and disease management. In the United States, the HIPAA legislation was enacted in 1996 to protect patients' personal information and applies to health plans, health care clearinghouses, health care providers, and employers. (see “Figure 4.5 – U.S. HIPAA Privacy Rule 2003” on page 13). Other countries have similar comprehensive laws that apply.

Figure 4.4 – ADMA Direct Marketing Code of Conduct

Privacy Principles

- Collection.
- Use and disclosure.
- Data quality.
- Data security.
- Openness.
- Access and correction.
- Identifiers.
- Anonymity.
- Transborder data flows.
- Sensitive information.

Figure 4.5 – U.S. HIPAA Privacy Rule 2003

The objective of HIPAA is to improve the efficiency and effectiveness of health care systems by facilitating electronic exchange of information and to recognize challenges to confidentiality of health information. HIPAA:

- Protects all individually identifiable health information.
- Defines and limits the circumstances in which an individual's health information may be used or disclosed.
- Requires written authorization for any use or disclosure of protected health information that is not for treatment, payment, or health care operations and is not otherwise permitted or required by the Privacy Rule.
- Limits uses and disclosures to the minimum necessary.
- Requires the development and implementation of policies and procedures that restrict access and uses.
- Requires to provide a notice of its privacy practices, including a point of contact for further information and for making complaints.
- Grants individuals the right to review and obtain a copy of their protected health information.
- Grants individuals the right to an accounting for the disclosures of their protected health information.
- Requires administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure.

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 are subject to significant embarrassment, damaged reputation, 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, or between trading partners that use and process personal information on a transnational level.

Figure 4.6 – Transborder Data Flow Issues for Data Subjects

- Language barriers.
- Control over data lost.
- Legal protection lost.
- Dispute not feasible.
- No access guarantees.
- Security unclear.

Examples of such cases include reservation systems, human resource functions in multinational companies, and transnational law enforcement cooperation (see “Figure 4.6 – Transborder Data Flow Issues for Data Subjects”).

International [OECD 1980 and APEC 2004] and regional [CoE 1981 and EU 1995] regimes create a framework for establishing trust. Commercial and nonprofit organizations should assure the personal information they collect, use, disclose, and retain remains in a secured and controllable location, where applicable standards are accepted and can be enforced.

Safe harbor agreements (such as the one in “Figure 4.7 – 2000 U.S./EU Safe Harbour Agreement”), mutual recognition of legal instruments, self-regulation, and in some cases, the reference to umbrella regulations like the OECD and CoE guidelines, provide a basis for privacy regimes to address international data transfers. The International Chamber of Commerce (ICC), the EU and other bodies provide model contracts for ensuring generally accepted privacy safeguards when businesses exchange personal data across borders.

Figure 4.7 – 2000 U.S./EU Safe Harbour Agreement

Self-certification of data holder to seven principles set by the U.S. Department of Commerce:

- Notice principle.
- Principle of choice.
- Onward transfer.
- Security.
- Data integrity.
- Access principle.
- Enforcement principle.

4.4 Privacy Control Framework

Basic privacy control framework activities include setting objectives, establishing policies and procedures, and establishing monitoring and improvement mechanisms. Objective setting is important to ensure an organization is aware of its privacy needs and can implement and monitor the required procedures on all levels. Organization policies and procedures are required to establish a structure for leading and coordinating operational and privacy-related efforts. Monitoring and improvement mechanisms are necessary to build on experience and to adapt objectives and direct the organization in a changing environment.

Applying Control Models to Privacy Management

Many organizations use control frameworks such as The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) 1992 *Internal Control — Integrated Framework* or its 2004 enhancement, *Enterprise Risk Management — Integrated Framework*. Organizations may also find other control frameworks, such as those listed in “Figure 4.8 – Widely Used Control Frameworks,” useful when developing an approach for analyzing and mitigating privacy exposures. Applying COSO's enterprise risk management (ERM) framework categories to privacy management and

Figure 4.8 – Widely Used Control Frameworks

- COSO's 1992 *Internal Control — Integrated Framework*.
- COSO's 2004 *Enterprise Risk Management — Integrated Framework*.
- CICA's 1995 Criteria of Control (CoCo).
- IT Governance Institute's 2005 Control Objectives for Information and related Technology (CobIT).
- ISO/International Electrotechnical Commission's (IECs) 27001 (BS 7799).

Figure 4.9 – Privacy Controls in the COSO ERM Framework

Internal Environment.	The privacy culture and tone of an organization, closely linked with its customer and social responsibility, is critical for the internal privacy risk and control environment. The internal environment includes the privacy code, implicit and explicit privacy policies, and organizational privacy culture, as established and communicated by senior management, all of which have to be aligned with applicable laws and regulations.
Objective Setting	Management needs to establish an organizational mission and vision from which privacy objectives and privacy policy can be derived, directly or indirectly. Organizational policies, job profiles, and individual performance plans may explicitly comprise privacy objectives.
Event Identification	Identifying potential internal and external privacy threats is mainly part of periodic and ongoing operational and information technology (IT) risk assessment.
Risk Assessment	Depending on an organization’s field of activity, privacy may be a more or less important aspect of operational and IT risk assessment. Hence, inherent and residual privacy exposures need to be well understood by operational management and staff as well as IT functions.
Risk Response	Privacy-enabled business processes, collection limitation, data security, contingency management, and data management measures avoid, accept, reduce, or share privacy-related risk.
Control Activities	Organizational policies, procedures, and structures that ensure that risk responses are carried out encompass elements like data security, access controls, integrity and contingency controls, privacy reviews, a privacy ombudsman, and many more.
Information and Communication	Relevant information needs to be expedited timely to allow effective control; instruments include observing privacy metrics and reporting on issues and their mitigation.
Monitoring	The privacy risk management system requires monitoring and adaptation as needed. An organization may appoint a privacy commissioner, maintain a data register, evaluate requests to access personal information records, and conduct privacy audits.

control provides a practical example for assessing privacy within an organization’s risk and control framework. (See “Figure 4.9 – Privacy Controls in the COSO ERM Framework.”)

The COSO ERM framework encompasses three dimensions: the organization, objectives, and risk management components. The organizational dimension describes the structural elements to be used for analyzing risk drivers and for implementation mechanisms or responsibilities. The objectives dimension helps to define the strategic, operational, reporting, and compliance objectives to be taken into account for privacy assessment. The risk management component dimension is instrumental for considering the privacy controls in an organization. Internal auditing can learn about potential areas for review when looking closer at this dimension.

Using a Privacy Maturity Model

An auditor needs criteria to evaluate where an organization stands with regard to its privacy practices. A capability maturity model such as the one in “Figure 4.10 – Generic Privacy Maturity Levels” on the following page, may be used to illustrate the development stage of privacy practices.

When an organization elects to employ a maturity model, internal auditing’s role is to support the development of the model, to gather and analyze data and communicate the results of an evaluation, and to validate self-assessments

performed by business lines or units. Internal auditing should also monitor the implementation of improvement plans.

A maturity model-based evaluation of privacy practices will either focus on maturity levels with regard to a set of privacy principles or specific criteria from a work program or benchmarking questionnaire. Depending upon the maturity of the organization’s existing practices, internal audit results may lead to:

- Measuring maturity.
- Raising awareness and influencing commitment.
- Assessing policies and procedures.
- Performing or supporting risk assessments.
- Recommending the establishment of a privacy task force or officer.
- Compliance audits.
- Evaluation of functions, processes, controls, products, and services.
- Establishment and/or validation of self-assessments.
- Recommendations, action plans, and implementation monitoring.

4.5 Determining Good and Bad Performers

The performance level of an organization can be determined by employing a maturity model as well as by benchmarking against general principles, a control framework, or best practices.

Figure 4.10 – Generic Privacy Maturity Levels

Initial	Activities are ad hoc, with: <ul style="list-style-type: none"> • No defined policies, rules, or procedures. • Eventually lower-level activities, not coordinated. • Redundancies and lack of teamwork and commitment.
Repeatable	The privacy policy is defined, with: <ul style="list-style-type: none"> • Some senior management commitment. • General awareness and commitment. • Specific plans in high-risk areas.
Defined	The privacy policy and organization are in place, with: <ul style="list-style-type: none"> • Risk assessments performed. • Priorities established and resources allocated accordingly. • Activities to coordinate and deploy effective privacy controls.
Managed	A consistently effective level of managing privacy, privacy requirements, and considerations is reflected in organization, with: <ul style="list-style-type: none"> • Early consideration of privacy in systems and process development. • Privacy integrated in functions and performance objectives. • Monitoring on an organizational and functional level. • Periodic risk-based reviews.
Optimizing	Continual improvement of privacy policies, practices, and controls, with: <ul style="list-style-type: none"> • Changes systematically scrutinized for privacy impact. • Dedicated resources allocated to achieve privacy objectives. • A high level of cross-functional integration and teamwork to meet privacy objectives.

— Source: Hargraves et al 2003

Indicators of Potential Privacy Issues

Potential privacy issues become visible when performing a high-level benchmark of an organization’s privacy practices against each set of basic privacy principles. For example, the eight OECD principles in “Figure 4.11 – Privacy Issue Indicators” allow such a quick analysis:

Figure 4.11 – Privacy Issue Indicators

Principle	Privacy Issue Indicator
Collection Limitation	There is no legal basis and no explicit consent for data collection.
Data Quality	Adequacy and correctness of data is never reviewed.
Purpose Specification	Purpose of data collection is not clearly defined.
Use Limitation	Personal information is used for other purposes than initially foreseen, lacking legal basis or consent.
Security Safeguards	Personal information not adequately protected against damage, loss, or disclosure.
Openness	Policies, practices, and means for processing personal data are not transparent.
Individual Participation	Individuals lack the practical opportunity to get information on their personal information that is being processed and retained.
Accountability	The organization has accountability for establishing and enforcing controls and processes.

Privacy Best Practices

A broad variety of best practices can be derived from existing privacy frameworks, research, and guidance from organizations like the OECD, Council of Europe, EU Commission, AICPA, CICA, and many industry associations. Several of the following privacy practices have proven to support good privacy management and to prevent disappointing surprises:

- Performing adequate and regular privacy risk assessments.
- Establishing a privacy ombudsman, officer, or organization to be available to act as the focal point for the coordination of privacy-related activities and the handling of complaints and issues.
- Developing awareness around key data handling and identity theft risks.
- Masking personal identification numbers, such as Social Security numbers, and other sensitive information when possible.
- Supervising and training call center staff to prevent social engineering and similar risks.
- Managing marketing lists and all third-party vendor relationships effectively.
- Creating awareness of Web, and e-mail vulnerabilities.
- Developing record retention and destruction policies.
- Implementing a data classification scheme based on the sensitivity and data mapping.
- Conducting risk assessments of access controls, physical security access restrictions, and change controls.
- Implementing intrusion detection and prevention technologies.

- Completing penetration testing and independent testing/review of key controls, systems, and procedures.

Limiting data collection to operationally necessary data, anonymizing personal information, using security technologies like encryption, and using opt-in and opt-out mechanisms also help individuals gain trust in the organization and help an organization to avoid or mitigate privacy risk. Moreover, privacy audits, seals, and certifications show an organization's commitment to a set framework and level of performance. Privacy reporting establishes transparency and additional trust in an organization's commitment to adequate treatment of personal data (see "Figure 4.12 – Good Privacy Practices").

Figure 4.12 – Good Privacy Practices

- Build consumer confidence.
- Protect the integrity of your organization's brand.
- Increase customer loyalty.
- Contribute to the bottom line.

— Source: Industry Canada

Auditing the organization's privacy practices involves risk assessment, engagement planning and performance, communication of results, and follow-up. However, there are additional aspects the CAE should take into account, including possible privacy breaches, staff management, and record retention issues. Many of these aspects are covered by professional practices of the internal, external, and IT audit professions. The key issues and methodologies are outlined in this chapter.

5.1 Internal Auditing's Role in the Privacy Framework

The IIA's PA 2100-8: Internal Auditing's Role in Evaluating an Organization's Privacy Framework outlines internal audit activities related to an organization's privacy framework. In today's business environment, privacy controls are legal and business requirements, and generally accepted policies and practices are evolving. An organization's governing body is responsible for establishing an appropriate privacy framework, and internal auditing can evaluate that framework, identify significant risks, and make appropriate recommendations. When evaluating an organization's privacy framework, internal auditors should consider the following:

- Laws and regulations in all jurisdictions in which business is conducted.
- Internal privacy policies and guidelines.
- Privacy policies intended for customers and the public.
- Liaising with in-house legal counsel to understand legal implications.
- Liaising with information technology specialists and business process owners to understand information security implications.
- The maturity of the organization's privacy controls.

The auditor's role includes conducting privacy risk assessments and providing assurance over privacy controls across the organization. Typical areas that internal auditing may review include:

- Management oversight.
- Privacy policies and controls.
- Applicable privacy notices.
- Types and appropriateness of information collected.
- Systems that process personal information.
- Collection methodologies.
- Uses of personal information according to stated intent, applicable laws, and other regulations.
- Security practices covering personal information.

When internal auditors assume a portion of the responsibility for developing and implementing a privacy program, their independence may be impaired. For this reason, and due to the possible need for sufficient technical and legal expertise, third-party experts may be required.

5.2 Activity Planning

The IIA's Standard 2010: Planning requires the CAE to set up a risk-based audit plan. PA 2010-1: Planning and 2010-2:

Linking the Audit Plan to Risk and Exposures detail further that audit universe, business objectives, risk, and controls have to be taken into account. All of these can be influenced by privacy objectives and risks.

More specific is PA 2100-6: Control and Audit Implications of E-commerce Activities, which states that an internal auditor should take disclosure of confidential business information, privacy violations, and reputation damage into account during audit planning and risk assessment. Legal issues such as increasing regulations throughout the world to protect individual privacy, enforceability of contracts outside the organization's country, and tax and accounting issues are some of the more critical risk and control issues to be addressed by the internal auditor. Accordingly, PA 2100-9: Application Systems Review recommends covering data risks relating to completeness, integrity, confidentiality, privacy, accuracy, and timeliness in audit planning.

5.3 Prioritizing and Classifying Data

An organization's private data can be considered a corporate asset, and its value can be positive or negative based on the control exercised over it. Well-controlled and appropriately used data can enhance an organization's worth, providing additional value to its customers. Disclosed personal data becomes a liability, reducing customer confidence and increasing the risk of legal and regulatory activity. Management may be reluctant to assign monetary values to privacy until it is lost.

A corporate classification program for privacy-protected data will assist in prioritizing the data. Assigning a sensitivity level — such as proprietary, confidential, or public — to data assists in evaluating the appropriateness of the controls over the technology and business processes that handle it. The auditor can ask the following questions:

- What are the regulatory penalties for mishandling privacy protected data? What legal recourse would the impacted individuals have?
- How has data ownership been assigned, and have appropriate controls been established in handling the data?
- Has the data been classified? Are the levels of classification appropriate for ensuring adequate privacy controls?
- 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 remediate 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, applications, and business processes.

Legal and Organizational Risks

Compliance with applicable laws and regulations is the foundation of most privacy programs. An attorney who is well-versed in privacy can champion privacy compliance, assisting in the design of a compliant privacy program, review of contracts with third parties to ensure appropriate privacy controls, and counsel in response to a privacy disclosure incident. Because privacy laws and regulations continue to evolve through actions of courts and regulators on an almost daily basis, an organization may seek to obtain services from a legal professional with specialization in the organization's industry.

Every organization should also designate an individual who is the primary coordinator or contact and has the principal responsibility for privacy issues. In smaller organizations, this responsibility may be part of the normal duties of the organization's legal counsel, compliance officer, human resources manager, or information security officer. In organizations that handle financial or health information as part of their core business, an individual dedicated to this function could be justified, or may be required by laws governing the industry. Many organizations have established a chief privacy officer (CPO), who reports directly to the chief executive or board of directors. An individual at this level can provide the awareness and advocacy needed to ensure that privacy risks are identified and communicated and that sufficient resources are allocated to address them.

As important to the organization as protecting privacy is the handling of privacy breach incidents. The primary privacy contact should coordinate a privacy incident response team that acts as a liaison to operational, legal, administrative, and technology areas within the organization, as well as to the potential claimants, the press, and law enforcement.

Without the appropriate tone at the top and strong privacy leadership, the organization's privacy program may be starved for resources and buried within the organizational structure. These conditions would minimize the privacy program's effectiveness and contribute to the risk of non-compliance.

Some legal and organizational questions to ask when planning a privacy audit include:

- Who are the designated privacy contacts? What percentage of their time is devoted to privacy issues? Do they have sufficient 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?

- Does the organization have a plan to respond to a privacy incident? Are the appropriate people included in the plan? Is the plan up-to-date?
- How involved are privacy contacts in the evaluation of new technologies and programs that impact privacy issues?

Infrastructure Risks

A basic principle of information security is to provide confidentiality, integrity, and availability of data, which overlaps many of the goals of a privacy program. Privacy relies on the controls implemented by information security; not all information security addresses privacy. An audit of a privacy program will necessarily involve significant review of information security controls. The toughest part simply may be identifying how the protected information flows in and out of 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, stored on a magnetic disk, printed out and put in a filing cabinet, backed up on an optical disk, and later sent off site on magnetic tape. Each time the data moves and changes format, the vulnerability of the data changes.

Shredders, encryption, locked vaults, and lockers all play a role as countermeasures to leaking data. Auditors should review the life cycle of personal information the organization is handling and determine if it is handled with the appropriate care along each step.

For example, how is encryption used in handling data? The auditors should trace data both in transit over public and private networks and data media handled by courier. Auditors should also follow up on stored data in production as well as in back-up and disaster recovery environments.

Additionally, auditors should ask how many times the data is converted from one form to another, and track data as it is converted from paper to packets to tape to paper to tape to magnetic disks. They should determine whether the data is being transferred or copied and whether the post-transfer residual data is 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 use a mix of in-house developed software, customized commercial off-the-shelf (COTS) software, and supporting middleware and operating systems to process, share, and distribute their data.

After the auditor identifies the automated processes, very basic security questions need to be addressed regarding any

application that handles private information:

- Were privacy issues identified in the requirements defining the application?
- Have data classification standards been implemented in the application to ensure appropriate controls over the data and information?
- How was the implementation of the requirements validated in development and deployment of the application?
- How does the application authorize and authenticate users?
- What sort of user roles does the application have? What are their authorizations?
- How is user access to the data tracked and logged?
- Are there external interfaces to other applications? Do these applications give an equivalent level of control over the data?
- Who is responsible for maintenance and upgrading the applications and the underlying database?
- Who responds to potential security issues and ensures that security bugs are tested and patched? Who is responsible for the general security of the application?
- In development and testing of applications, is test data used? Has it been appropriately anonymized? If not, are the controls in the test environment equivalent to controls in the production environment?

Business Process Risks

Despite technicians' efforts to guard, encrypt, and otherwise secure private data, the business process will eventually necessitate that the data is used for its intended purpose. As the data is used, it is important that the individuals treat it with the level of care corresponding to its data classification. Measures to protect printed information should follow the same principles used to classify and protect electronic data. At minimum, desks should be clean, and drawers and filing cabinets should be locked. Discretion should be used in areas open to the public.

5.5 - Preparing the Engagement

According to The IIA's PA 2100-8: Internal Auditing's Role in Evaluating an Organization's Privacy Framework, internal auditors should typically review the type and appropriateness of the information collected by the organization, collection methodologies, and use of the information collected according to stated intent, law, and other regulations.

Information Systems Audit and Control Association (ISACA) Guideline 31 - Privacy references CoBIT 4.0's control objectives ME3 (Ensure Regulatory Compliance) and DS5 (Ensure Systems Security). Management's detailed control objectives with regard to regulatory compliance are to ensure identification of relevant laws and regulations (ME3.1), to ensure evaluation of compliance (ME3.3), and to provide positive assurance of compliance (ME3.4). The relevant

primary information criteria are effectiveness, compliance, confidentiality, and integrity. The guideline contains a brief checklist for measuring an organization's privacy framework against the OECD Privacy Guideline's principles as well as steps to be performed in a privacy-related audit and criteria for reporting (see "Figure 5.1 – Privacy Audit Program Sections").

Approaches to developing a privacy audit program are identified in several publications. An intuitively sequenced model for an audit program structure, which builds on the OECD criteria, is provided in *Privacy Handbook* (Marcella 2003) and is based on the 2001 Canadian PIPEDA principles by the Information and Privacy Office of Ontario. In comparison, *Privacy – Assessing the Risk* (Hargraves et al, 2003) presents an exhaustive program with a more technology-oriented structure. Detailed criteria and explanations around the 10 AICPA/CICA principles are contained in the AICPA/CICA's 2004 *Generally Accepted Privacy Principles – A Global Privacy Framework*. Additional information on these and other audit program guidance is listed in the Appendix.

Figure 5.1 – Privacy Audit Program Sections

- Accountability.
- Purpose identification.
- Collection.
- Consent.
- Use, disclosure, and retention.
- Accuracy.
- Safeguards.
- Openness.
- Individual access.
- Challenging compliance.

Privacy Assessments

Several legal and regulatory regimes require or recommend privacy assessments. Many organizations also realize an operational, internal control, and risk management-driven need to review the adequacy of privacy policies and their effectiveness. Existing assessment models provide extensive guidance for setting up audit work programs. The AICPA/CICA's GAPP and Privacy Framework provide a comprehensive program that can be used by any organization to conduct a privacy assessment. This document is available free for download at www.infotech.aicpa.org/Resources/Privacy/.

The objectives of a privacy assessment need to be established first. For example, objectives can be:

- To determine inherent and residual privacy-related risks.
- To provide assurance on controls over privacy risks.
- To verify adherence to a set privacy standard.

The United Kingdom Information Commissioner's *Data Protection Audit Manual* describes general privacy audit processes: external and internal, adequacy and compliance, and vertical (functional) or horizontal (process). Auditors may begin an assessment by scoping the audit areas — the whole

GTAG — Auditing Privacy — 5

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 (examples are listed in the Appendix) 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 auditing should review both the sufficiency of the audits performed and the effectiveness of the follow-up mechanism in place.

Understand Personal Data Processing

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

- Obtain a comprehensive understanding of the personal data held, its use by the organization, its handling through technology, and the regulation of its processing.
- Identify the rules that govern the data the organization is processing.
- Interview the individual(s) responsible for the organization's privacy policy and its enforcement 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.
- Determine regulations and governmental bodies responsible for enforcing privacy rules. Ask the privacy officer how such rules are codified in the organization's policies and procedures.
- Identify the customers', employees', and business partners' protected data that the organization collects

- Identify how the data is shared with third parties — the formal and informal means by which personal data is shared within the organization and with other entities to identify threats, vulnerabilities, and overall risk to the data.

Identify the Threats

A threat is an actor that uses a vulnerability to exploit an asset. For the purposes of privacy management, the asset is the protected personal data. So, who or what is the threat? The threat is the individual or process that, intentionally or not, makes an organization's private data public.

The hacker employed by organized crime is a romantic image, and could be a legitimate threat. However, the networked hacker many time zones away won't make it into a chief executive officer's trash can, manager's briefcase, or open filing cabinet. Empirically verified, the threats posed by employees, contract or temporary workers, competitors, developers, janitors, and maintenance staff — those who often have authorized access to stores of confidential information — are most relevant. Whether through malice or carelessness, these individuals have the ability to make most any type of business data public. If privacy protected data is shared with business partners and contractors, the additional threats to and within their operations and processes should be evaluated.

Auditors should identify the threats to the organization's data through research, benchmarking, and brainstorming, and rank them according to the likelihood of occurrence and impact. If they are successful, this effort creates a matrix that correlates the risks with privacy asset (see "Figure 5.2 – Privacy Audit Assessment Matrix"). Assigning values to threats and assets highlights where the strongest controls or countermeasures should be, and the areas in which the auditors should focus to identify vulnerabilities.

Identify the Controls and Countermeasures

To determine what the organization is doing to protect personal data from the worst threats, auditors must dig into the active controls used in the organization's privacy program. Common steps to identify the controls include:

- **Requesting and reviewing the documentation.**
Review the privacy program as it is implemented in policies, procedures, and memoranda. How do the

Figure 5.2 - Privacy Audit Assessment Matrix

Asset	Threat	Impact	Controls	Audit Work	Conclusion
Application	Loss	Financial	Preventive	Testing	Well controlled
Database	Damage	Reputation	Compensating	Interviews	Improvement required
File type	Unavailability	Compliance	Detective	Observation	Inadequate control
Relationship	Disclosure	Operational	
...	Maturity models can provide an alternative

policies match up with the high-risk areas defined in the privacy audit assessment matrix? 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 data processing in action.** The gap between the written policy and the operational action can be significant. Sit with the employees on the front lines and determine if they are aware of the impact of their actions in handling personal data. Also, determine if there are undocumented controls in place, and if the spirit as well as the letter of the privacy program motivates staff's decisions.
- **Reviewing third-party contracts and contacts.** The depth of the review will depend on how the contractors and the data handled by them rank in the threat matrix, but the auditor should perform, at minimum, a review for language compliant with applicable laws and regulations. If audit clauses are included, are they exercised with appropriate frequency and depth?

The IIA's PA 2100-13: Effect of Third Parties on an Organization's IT Controls states that using a third-party provider's controls wholly, or in conjunction with the organization's own controls, will impact the organization's ability to achieve its control objectives. A lack of controls and/or weakness in control design, operation, or effectiveness could lead to such things as loss of 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.

Prioritization

By this point, the potential high-impact risks should come into sharper focus, and 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 *Professional Practices Framework*: when the organization's objectives, the types of data handled, and the legal framework are understood, an audit program including scope, objectives, and timing of the audit is to 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.

Assessing Privacy Management

The AICPA/CICA developed a set of criteria for each of the 10 privacy principles contained in its GAPP framework. As an example, the management principle (see "Figure 5.3 –

AICPA/CICA Privacy Management Criteria") can be used for reviewing and assessing the effectiveness of privacy management within an organization. The principle requires that an entity define, document, communicate, and assign accountability for its privacy policies and procedures. To assess privacy management, internal auditors should review policies and communications as well as procedures and controls.

Figure 5.3 – AICPA/CICA Privacy Management Criteria

Principle 1: The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

Policies and Communications

- Privacy policies.
- Communication to internal personnel.

Procedures and Controls

- Review and approval.
- Consistency of privacy policies and procedures with laws and regulations.
- Consistency of commitments with privacy policies and procedures.
- Infrastructure and systems management.
- Supporting resources.
- Qualifications of personnel.
- Changes in business and regulatory environments.

Test Work Methodologies

Once the general management controls are assessed, the test work needed should become clear. Potential test methods beyond the usually applied techniques include vulnerability assessments and penetration tests, physical control tests, or 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 saucier 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 identification of 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 will need to acquire, either through contract or training. An excellent guide on the subject is the *Open Source Security Testing Methodology Manual* from the Institute of Security and Open Methodologies.

Physical Control Tests

Protected information is not limited to digital data. If your modeled threat has access to the building, all the encryption, firewalls, and patched databases in the world can't keep that individual from fishing 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 private information being disposed of according to policy and procedures?
- Are documents stored securely prior to disposal or shredding?
- Are working documents with private data stored securely?
- Are documents or monitors that display confidential information viewable by nonauthorized personnel?
- Are workstations locked when unattended?
- Is the application of privacy controls consistent across various departments?

Social Engineering Tests

Social engineering 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 the controls regarding release of private data. In other words, can an individual obtain personal data by simply asking for it? The auditor could impersonate executives, network administrators, or other authorized users to “con” or “sweet talk” passwords or private 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 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 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

In accordance with The IIA's Standard 2400: Communicating Results, an audit report should be issued to the client after a privacy audit assignment. The CAE should then monitor the status of implementation improvements agreed to by the audit client in the report.

Many privacy assessments 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. For further guidance in this area, refer to The IIA's PA 2400-1: Legal Considerations in Communicating Results and PA 2100-5: Legal Considerations in Evaluating Regulatory Compliance Programs, which can be found in the Guidance section of The IIA's Web site, www.theiia.org.

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

- Getting all of the participants involved. 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 internal legal counsel has reviewed the proposed audit plan and draft audit report before issuance to ensure that compliance considerations are addressed properly.

IIA Standard 2500 and 2600, as well as ISACA Standard 8, state that subsequent to an audit, a follow-up of management's actions or acceptance of risk is required to ensure effective mitigation of organizational risk.

5.8 Privacy and Audit Management

The IIA's *Professional Practices Framework* reminds auditors to take privacy regulations and risks into account when planning, performing, and reporting assurance and consulting assignments. Professional bodies, legislators, and supervisory authorities issue a broad variety of guidance and regulations.

Due to the increasing risk of reputation damage and litigation, the CAE has to take a significant spectrum of privacy issues and ramifications into account when managing the audit function. Key areas of concern are the staff management process; audit planning; collecting, handling, and storing information when performing and reporting audit results; and potential data leaks. Section eight of ISACA's Guideline 31 – Privacy also lists generic controls and areas of concern, providing useful criteria for the CAE to use when managing the audit function.

An organization needs to use due care when delegating substantial discretionary authority to individuals (refer to The IIA's PA 2100-5: Legal Considerations in Evaluating Regulatory Compliance Programs). When screening applicants for employment at all levels, care should be taken to ensure that the company does not infringe upon employee and applicant privacy rights.

When hiring auditors, there is even a greater need for due diligence to ensure that newly hired auditors act in accordance with relevant laws and policies when using personal information during assurance or consulting engagements (refer to The

IIA's PA 2300-1: Internal Auditing's Use of Personal Information in Conducting Audits in the Appendix, page 27.) Internal auditors must 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. Examples of potential pitfalls are listed in "Figure 5.4 – What Can Go Wrong: Caveats for CAEs." Before initiating an audit, the auditors should investigate these issues and request advice from in-house legal counsel, if needed. Finally, internal auditors should consider related privacy regulations, regulatory requirements, and legal considerations when reporting information outside the organization, as recommended by The IIA's PA 2440-2: Communications Outside the Organization.

Figure 5.4 – What Can Go Wrong: Caveats for CAEs

- An informal background check with a new hire's former employer is determined illegal.
- Privacy risks are insufficiently covered in the audit department's annual planning.
- At the airport, a staff member checks in his suitcase, with a laptop inside.
- Human resource records are stored unencrypted on the department's local area network (LAN) drive.
- An employee resigns, taking a copy of the audit database with him.
- A laptop is stolen from an employee's suitcase in a hotel room.
- An auditor's trunk, which contains confidential data is burgled at the airport.
- A hard disk containing personal information is stolen from a computer in the staff room.
- Human resource files are piling up in an auditor's workspace.

GTAG — Top 10 Privacy Questions CAEs Should Ask — 6

1. What privacy laws and regulations impact the organization?
2. What type of personal information does the organization collect?
3. Does the organization have privacy policies and procedures with respect to collection, use, retention, destruction, and disclosure of personal information?
4. Does the organization have responsibility and accountability assigned for managing a privacy program?
5. Does the organization know where all personal information is stored?
6. How is personal information protected?
7. Is any personal information collected by the organization disclosed to third parties?
8. Are employees properly trained in handling privacy issues and concerns?
9. Does the organization have adequate resources to develop, implement, and maintain an effective privacy program?
10. Does the organization complete a periodic assessment to ensure that privacy policies and procedures are being followed?

7.1 The IIA’s Professional Practices Framework

Specific privacy-related guidance can be found in the The IIA’s *Code of Ethics*, *International Standards for the Professional Practice of Internal Auditing*, 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

**Figure 7.1 – Privacy-related IIA Practice Advisories
(in brackets: secondary)**

IIA PA	Title
(1130.A1-2)	Internal Audit Responsibility for Other (Nonaudit) Functions
(2010-1)	Planning
(2010-2)	Linking the Audit Plan to Risks and Exposures
(2050-1)	Coordination
2100-2	Information Security
(2100-5)	Legal Considerations in Evaluating Regulatory Compliance Programs
(2100-6)	Control and Audit Implications of E-commerce Activities
2100-8	Internal Auditing’s Role in Evaluating an Organization’s Privacy Framework
2100-12	Outsourcing of IS Activities to Other Organizations
2100-13	Effect of Third Parties on an Organization’s IT Controls
2300-1	The Internal Auditor’s Use of Personal Information in Conducting Audits
2330-1	Recording Information
2330.A1-1	Control of Engagement Records
2330.A1-2	Legal Considerations in Granting Access to Engagement Records
2400-1	Legal Considerations in Communicating Results
2440-1	Recipients of Engagement Results
2440-2	Communications Outside the Organization
(2440-3)	Communicating Sensitive Information Within and Outside of the Chain of Command

Figure 7.2 – IIA Practice Advisory 2100-8: Internal Auditing's Role in Evaluating an Organization's Privacy Framework

Related Standard

2100 – Nature of Work

The internal audit activity should evaluate and contribute to the improvement of risk management, control, and governance processes using a systematic and disciplined approach.

Nature of this Practice Advisory:

Internal auditors should consider the following suggestions when evaluating an organization's activities related to its privacy framework. This guidance is not intended to represent all procedures necessary for a comprehensive assurance or consulting engagement related to the privacy framework, but rather a recommended core set of high level auditor responsibilities to complement related board and management responsibilities.

1. Concerns relating to the protection of personal privacy are becoming more apparent, focused, and global as advancements in information technology and communications continually introduce new risks and threats to privacy. Privacy controls are legal requirements for doing business in most of the world.
2. Privacy definitions vary widely depending upon country, culture, political environment, and legal framework. Privacy can encompass personal privacy (physical and psychological); privacy of space (freedom from surveillance); privacy of communication (freedom from monitoring); and privacy of information (collection, use, and disclosure of personal information by others). Personal information generally refers to information that can be associated with a specific individual, or that has identifying characteristics that might be combined with other information to do so. It can include any factual or subjective information, recorded or not, in any form or media. Personal information might include, for example:
 - Name, address, identification numbers, income, or blood type;
 - Evaluations, comments, social status, or disciplinary actions; and
 - Employee files, credit records, loan records.
3. Privacy is a risk management issue. Failure to protect privacy and personal information with the appropriate controls can have significant consequences for an organization. For example, it can damage the reputation of individuals and the organization, lead to legal liability issues, and contribute to consumer and employee mistrust.
4. There are a variety of laws and regulations developing worldwide relating to the protection of personal information. As well, there are generally accepted policies and practices that can be applied to the privacy issue.
5. It is clear that good privacy practices contribute to good governance and accountability. The governing body (e.g., the board of directors, head of an agency or legislative body) is ultimately accountable for ensuring that the principal risks of the organization have been identified and the appropriate systems have been implemented to mitigate those risks. This includes establishing the necessary privacy framework for the organization and monitoring its implementation.
6. The internal auditor can contribute to ensuring good governance and accountability by playing a role in helping an organization meet its privacy objectives. Internal auditors are uniquely positioned to evaluate the privacy framework in their organization and identify the significant risks along with the appropriate recommendations for their mitigation.
7. In conducting such an evaluation of the privacy framework, internal auditors should consider the following:
 - The various laws, regulations, and policies relating to privacy in their respective jurisdictions (including any jurisdiction where the organization conducts business);
 - Liaison with in-house legal counsel to determine the exact nature of such laws, regulations, and other standards and practices applicable to the organization and the country/countries in which it does business;
 - Liaison with information technology specialists to ensure information security and data protection controls are in place and regularly reviewed and assessed for appropriateness;
 - The level or maturity of the organization's privacy practices. Depending upon the level, the internal auditor may have differing roles. The auditor may facilitate the development and implementation of the privacy program, conduct a privacy risk assessment to determine the needs and risk exposures of the organization, or may review and provide assurance on the effectiveness of the privacy policies, practices, and controls across the organization. If the internal auditor assumes a portion of the responsibility for developing and implementing a privacy program, the auditor's independence may be impaired.
8. Typically, internal auditors could be expected to identify the types and appropriateness of information gathered by their organization that is deemed personal or private, the collection methodology used, and whether the organization's use of the information so collected is in accordance with its intended use and the laws, in the areas that the information is gathered, held and used.
9. Given the highly technical and legal nature of the topic, the internal auditor should ensure that the appropriate in-depth knowledge and capacity to conduct any such evaluation of the privacy framework is available, using third-party experts, if necessary.

Origination date: Feb. 12, 2004

Figure 7.3 – IIA Practice Advisory 2300-1: Internal Auditing's Use of Personal Information in Conducting Audits.**Related Standard****2300 – Performing the Engagement**

Internal auditors should identify, analyze, evaluate, and record sufficient information to achieve the engagement's objectives.

Nature of this Practice Advisory

Internal auditors should consider the following suggestions when considering the use of personal information in the conduct of an assurance or consulting engagement. This practice advisory is not intended as comprehensive guidance related to the use of personal information, but rather a reminder of the importance of its appropriate use in accordance with the laws and policies of the relevant jurisdiction where the audit is being conducted and where the organization conducts business.

1. Concerns relating to the protection of personal privacy and information are becoming more apparent, focused, and global as advancements in information technology and communications continually introduce new risks and threats to privacy. Privacy controls are legal requirements for doing business in most of the world.
2. Personal information generally refers to information that can be associated with a specific individual, or that has identifying characteristics that might be combined with other information to do so. It can include any factual or subjective information, recorded or not, in any form or media. Personal information might include, for example:
 - Name, address, identification numbers, income, or blood type;
 - Evaluations, comments, social status, or disciplinary actions; and
 - Employee files, credit records, loan records.
3. For the most part, laws require organizations to identify the purposes for which personal information is collected, at or before the time the information is collected; and that personal information not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
4. It is important that internal auditors understand and comply with all laws regarding the use of personal information in their jurisdiction and those jurisdictions where their organization conducts business.
5. The internal auditor must understand that it may be inappropriate, and in some cases illegal, to access, retrieve, review, manipulate, or use personal information in conducting certain internal audit engagements.
6. The internal auditor should investigate issues before initiating audit effort and seek advice from in-house legal counsel if there are any questions or concerns in this respect.

Origination date: Feb. 12, 2004

7.2 Other Auditing Standards and Methodology

ISACA Guidance

Privacy-related guidance can be found in:

- CobiT 4.0 ME3 - Ensure Regulatory Compliance.
- CobiT 4.0 DS5 - Ensure Systems Security.
- ISACA Guideline 31 - Privacy.
- CobiT 3.2 Audit Guidelines - PO8.

AICPA/CICA Guidance

The AICPA/CICA GAPP is a comprehensive framework that provides criteria organizations can use to effectively implement, manage, or assess their privacy program. Each of the following 10 principles is supported by objective and measurable criteria contained within the framework:

1. **Management** – The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice** – The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and Consent** – 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.
4. **Collection** – The entity collects personal information only for the purposes identified in the notice.
5. **Use and Retention** – 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.
6. **Access** – The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to Third Parties** – 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.
8. **Security for Privacy** – The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality** – The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and Enforcement** – The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

AICPA/CICA Management Principle Criteria

The AICPA/CICA management principle supports the assessment of an organization's privacy management practices. The

complete document containing all 10 principles and criteria is available for free download at infotech.aicpa.org/Resources/Privacy.

Management principle

The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

Privacy management criteria:

1.1. Policies and Communications

1.1.0 Privacy Policies

- The entity defines and documents its privacy policies with respect to:
 - Notice.
 - Choice and consent.
 - Collection.
 - Use and retention.
 - Access.
 - Onward transfer and disclosure.
 - Security.
 - Quality.
 - Monitoring and enforcement.

1.1.1 Communication to Internal Personnel

Privacy policies and the consequences of non-compliance with such policies are communicated at least annually to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.

1.1.2 Responsibility and Accountability for Policies

Responsibility and accountability are assigned to a person or group for documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such persons or groups and their responsibilities are communicated to internal personnel.

1.2 Procedures and Controls

1.2.1 Review and Approval

Privacy policies and procedures and changes thereto are reviewed and approved by management.

1.2.2 Consistency of Privacy Policies and Procedures with Laws and Regulations

Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever there are changes to such laws and regulations. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.

1.2.3 Consistency of Commitments with Privacy Policies and Procedures

Entity personnel or advisors review contracts for consistency with privacy policies and procedures and address any inconsistencies.

1.2.4 Infrastructure and Systems Management

Entity personnel or advisors review the design, acquisition, development, implementation, configuration, and management of:

- Infrastructure,
- Systems,
- Applications,
- Web sites, and
- Procedures,

and changes thereto for consistency with the entity's privacy policies and procedures and address any inconsistencies.

1.2.5 Supporting Resources

Resources are provided by the entity to implement and support its privacy policies.

1.2.6 Qualifications of Personnel

The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.

1.2.7 Changes in Business and Regulatory Environments

For each jurisdiction in which the entity operates, the effect on privacy of changes in the following factors is identified and addressed:

- Business operations and processes.
- People.
- Technology.
- Legal.
- Contracts, including service-level agreements. Privacy policies and procedures are updated for such changes.

7.3 Selected Monographs

AICPA/CICA: *Generally Accepted Privacy Principles – A Global Privacy Framework* (2006)

Carey: *Data Protection: A Practical Guide to UK and EU Law* (Oxford University Press, 2004)

Cate: *Privacy in the Information Age* (Brookings, 2001)

CICA: *20 Questions Directors Should Ask About Privacy* (CICA, 2002)

CICA: *Privacy Compliance: A Guide for Organizations & Assurance Practitioners* (CICA, 2004)

Hargraves et al: *Privacy – Assessing the Risk* (IIA RF, 2003)

Karol, T.J.: *A Guide to Cross-border Privacy Assessments* (ITGI, 2001)

Marcella/Stucki: *Privacy Handbook* (Wiley, 2003)

Margulis: *Contemporary Perspectives on Privacy: Social, Psychological, Political* (Blackwell, 2003)

OECD: *Privacy Online. OECD Guidance on Policy and Practice* (OECD, 2003)

Solove/Rotenberg/Schwartz: *Information Privacy Law* (Aspen, 2005)

Westby, Jody R. (Ed.): *International Guide to Privacy* (ABA, 2004)

7.4 Global and Regional Governmental Resources

Council of Europe

www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection

The Council of Europe's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" was opened for signature on Jan. 28, 1981. To this day, it remains the only binding international legal instrument with a worldwide scope of application in this field. It is open to any country, including countries that are not members of the Council of Europe.

European Commission Data Protection Pages

www.europa.eu.int/comm/justice_home/fsj/privacy

Developments of the internal market and the so-called "information society" increase the cross-frontier flows of personal data among member states of the EU. To remove potential obstacles to such flows and to ensure a high level of protection within the EU, data protection legislation has been harmonized. This Web site provides links to EU expert groups and national privacy commissioners.

OECD's Information Security and Privacy Pages

www.oecd.org/sti/security-privacy

The OECD Working Party on Information Security and Privacy promotes a global, coordinated approach to policy-making in these areas to help build trust online.

OECD Privacy Statement Generator

www.oecd.org/sti/privacygenerator

The Generator, which has been endorsed by the OECD's 30 member countries, offers guidance on compliance with the

Privacy Guidelines and helps organizations develop privacy policies and statements.

7.5 Regional and National Resources

See *ITAudit* for more US Health & Human Services

Privacy Committee

www.aspe.hhs.gov/datacncl/privacy

The U.S. Health & Human Services Privacy Committee ensures attention to privacy as a fundamental consideration in collection and use of personally identifiable information.

U.S. Federal Trade Commission Privacy Initiatives

www.ftc.gov/privacy/index.html

Privacy is a central element of the Federal Trade Commission's consumer protection mission: The FTC is educating consumers and businesses about the importance of personal information privacy, including the security of personal information.

U.S. Health Privacy Project

www.healthprivacy.org

The Health Privacy Project is dedicated to raising public awareness of the importance of ensuring health privacy to improve health care access and quality, both on an individual and a community level.

U.S. Health & Human Services Office for Civil Rights

HIPAA Pages

www.hhs.gov/ocr/hipaa

The U.S. Department of Health & Human Services' Office for Civil Rights medical privacy pages contain information on national standards to protect the privacy of personal health information.

U.S. National Institutes of Health HIPAA Pages

<http://privacyruleandresearch.nih.gov>

Part of the U.S. Department of Health & Human Services, the National Institutes of Health is the federal focal point for medical research in the United States. It provides standards for Privacy of Individually Identifiable Health Information; Final Rule.

7.6 Professional and Nonprofit Organizations

Computer Professionals for Social Responsibility

www.cpsr.org

CPSR is a global organization that promotes the responsible use of computer technology. Founded in 1981, CPSR educates policymakers and the public on a wide range of issues. CPSR has incubated numerous projects such as Privaterra, the Public Sphere Project, the Electronic Privacy Information Center, the 21st Century Project, the Civil Society Project, and the Computers, Freedom & Privacy Conference. Originally founded by U.S. computer scientists, CPSR now has members in more than 30 countries on six continents.

Electronic Privacy Information Center

www.epic.org

EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the U.S. First Amendment, and constitutional values.

AICPA/CICA Privacy Task Force

<http://infotech.aicpa.org/Resources/Privacy>

The AICPA and the CICA have formed the AICPA/CICA Privacy Task Force, which has developed the AICPA/CICA Generally Accepted Privacy Principles – A Global Privacy Framework.

Online Privacy Alliance

www.privacyalliance.org

The Online Privacy Alliance leads and supports self-regulatory initiatives to create an environment of trust that fosters the protection of individuals' privacy online and in electronic commerce.

International Conference of Data Protection and Privacy Commissioners

www.privacyconference2005.org

This site features the annual International Conference of Data Protection and Privacy Commissioners.

PrivacyExchange

www.privacyexchange.org

PrivacyExchange is an online global resource for consumer privacy and data protection. It contains a library of privacy laws, practices, publications, Web sites, and other resources concerning consumer privacy and data protection developments worldwide.

Japan Privacy Resource

www.privacyexchange.org/japan/japanindex.html

The Japan Privacy Resource has been designed and launched as a free service to all those engaged in privacy debates.

Privacy International

www.privacyinternational.org

Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world.

Platform for Privacy Preferences (P3P)

www.w3c.org/p3p/

Developed by the W3C, P3P is a standard that provides a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. P3P enhances user control by putting privacy policies where users can find

them, in a form users can understand and, most importantly, enables users to act on what they see.

7.7 More Internet Resources

Asia-Pacific Economic Cooperation

www.apec.org

The APEC Privacy Framework promotes a consistent approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.

Canadian Institute of Chartered Accountants

www.cica.ca

CICA has launched a comprehensive privacy initiative to raise awareness of privacy issues among both members and businesses. This initiative includes developing resources to educate businesses and members on the benefits of good privacy practices.

Consumers International

www.consumersinternational.org

Consumers International defends the rights of all consumers through empowering national consumer groups and campaigning at the international level.

European Data Protection Supervisor

www.edps.eu.int

The European Data Protection Supervisor is an independent supervisory authority responsible for monitoring the processing of personal data by the European Community institutions and bodies.

International Chamber of Commerce

www.iccwbo.org

Business leaders and experts drawn from the ICC membership establish the key business positions, policies, and practices on e-business, information technologies, and telecommunications through the Commission on E-Business, IT and Telecoms.

Institute for Security and Open Methodologies

www.isecom.org/osstmm

The Institute for Security and Open Methodologies provides the Open Source Security Testing Methodology Manual.

Quality-of-Life Policy Bureau, Cabinet Office, Government of Japan

www5.cao.go.jp/seikatsu/index.html

Provides details of the personal information protection law and related information as well as a counseling counter of personal information.

Japanese Information Processing Development Corp.

www.privacymark.org

Activities in the field of privacy and security include the operation of a system for granting Privacy and Personal Data Protection seals.

Office of the Privacy Commissioner

www.privacy.gov.au

The Australian Government's Office of the Privacy Commissioner is an independent organization that promotes an Australian culture that respects privacy.

International Association of Privacy Professionals

www.privacyassociation.org

IAPP is an association of privacy and security professionals. It defines and supports the privacy profession by being a forum for interaction, education, and discussion. IAPP issues a Certified Information Privacy Professional designation.

Privacy Commissioner of Canada

www.privcom.gc.ca

The Commissioner investigates complaints and conducts audits, publishes information about personal information-handling practices in the public and private sectors, conducts research into privacy issues, and promotes awareness and understanding of privacy issues.

National Telecommunications and Information Administration's Online Privacy Technologies Workshop 2000

www.ntia.doc.gov/ntiahome/privacy

The U.S. NTIA hosted a public workshop to examine technological tools and developments that can enhance consumer privacy online.

7.8 Glossary of Terms

Acceptable risk	The level of risk that management finds acceptable to a particular information asset. Acceptable risk is based on empirical data and supportive technical opinion that the overall risk is understood and that the controls placed on the asset or environment will lower the potential for its loss. Any remaining risk is recognized and accepted as an accountability issue.
Access	With respect to privacy, an individual's ability to view, modify, and contest the accuracy and completeness of personally identifiable information collected about him or her.
Alternative dispute resolution	Methods used to resolve disputes out of court, including negotiation, conciliation, mediation, and arbitration.
Aggregate	Data that is combined without releasing personally identifiable information.
Anonymity	A condition in which an individual's true identity is unknown.
Anonymization	Previously identifiable, now deidentified data for which a code or other link identifying the data subject no longer exists.
Authentication	The act of verifying the identity of a system entity (e.g., user, system, network node) and the entity's eligibility to access computerized information. Designed to protect against fraudulent logon activity. Authentication can also refer to the verification of the correctness of a piece of data.
Authorization	Approval of a transaction or action by the appropriate level of management.
Availability	Assurance that the systems responsible for delivering, storing, and processing information are accessible when needed, by those who need them, and that the information they provide are of acceptable integrity.
Biometrics	A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint.
Collection	Assembling of personal information through interviews, forms, reports, or other information sources.
Compliance	Adherence to the policies, procedures, guidelines, laws, regulations, and contractual arrangements to which the business process is subject.
Computerized file	Set of personal information stored and/or processed by an automated system.
Consent	An individual's agreement for the entity to collect, use, and disclose personal information in accordance with the privacy notice. Such agreement can be explicit or implied. Explicit consent is given either orally or in writing, is unequivocal, and does not require any inference on the part of the entity seeking consent. Implicit consent may reasonably be inferred from the action or inaction of the individual. (See <i>opt in</i> and <i>opt out</i> , below.)
Control	A policy, manual, or computerized procedure designed to provide reasonable assurance regarding achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.
Consumer information	Information about an individual's transactions and behavior in the marketplace.
Chief privacy officer	An individual assigned to ensure that a data controller's personal data is kept safe and, more importantly, customer satisfaction is kept high.
Data controller	Organizations or functions that control access to, and processing of, personal information.
Data matching	An activity that involves comparing personal data obtained from a variety of sources for the purpose of making decisions about the individuals to whom the data pertains.
Data mining	The practice of compiling, combining, and analyzing information about data subjects from a variety of data sources, usually for marketing purposes.

Data security	Protection of data from accidental or unauthorized modification, destruction, or disclosure through policies, organizational structure, procedures, awareness training, software, or hardware that ensure data is accurate, available, and accessed only by those authorized. Maintenance of confidentiality, integrity, and availability of information.
Data subject (individual)	The person about which personal data is collected.
Disclosure	The release, transfer, relay, provision of access to, or conveying of personal data to any individual or entity outside the data controller.
Dispute resolution	Includes all processes for resolving a conflict, from consensual to adjudicative, from negotiation to litigation.
Effectiveness	A control objective that specifies that information should be relevant and pertinent to the business process and delivered in a timely, correct, consistent, and usable manner.
Efficiency	A control objective that concerns the provision of information through the most productive and economical use of resources.
Enforcement	Mechanisms to ensure compliance and appropriate means of recourse by injured parties (also redress).
Entity	An organization that collects, uses, retains, and discloses personal information.
Fair information practices	A set of five principles — access, consent, enforcement, notice, and security — originating from the U.S. Privacy Act of 1974, designed to guide entities in their personal data processing practices.
Functionality	A control objective that specifies that a system should include all relevant capabilities.
Identification	The relating of personal information to an identifiable individual.
Identity theft	The deliberate use of another person’s name and other identifying information to commit theft or fraud or to access confidential information about an individual.
Individual (data subject)	The person about which personal data is collected.
Individually identifying information	Any single item or compilation of information that indicates or reveals the identity of an individual, either specifically (such as the individual’s name or Social Security number), or information from which the individual’s identity can reasonably be ascertained.
Information asset	Information in any form (e.g., written, verbal, oral, or electronic) upon which the organization places a measurable value. This includes information created by the data controller, gathered for the data controller, or stored by a data processor for external parties.
Information privacy	An individual’s right to control his or her personal information held by others.
Integrity	The property of data that has not been altered or destroyed in an unauthorized manner.
Location data	Information that can be used to identify an individual’s current physical location and to track location changes.
Manual file	Collection of personal information stored on noncomputerized media.
Nonroutine use	Use of information not for the purpose for which it was collected.
Notice	The informing of individuals of an entity’s data policies or practices prior to collecting their personal information.
Ombudsman	An advocate, or supporter, who works to solve problems between data subjects and data controllers or data processors.
Omnibus law	A law that applies in all respects.
Opt in	The explicit consent of the individual is required for personal information to be collected, used, retained, or disclosed by the entity.

GTAG — Appendix — 7

Opt out	Consent is implied, and the individual must explicitly deny consent if he or she does not want the entity to collect, use, retain, or disclose his or her personal information.
Outsourcing	The use and handling of personal information by a third party that performs a business function for the entity.
Personal data (personal information, personally identifiable information)	Information about an identified or identifiable individual that includes any factual or subjective information, recorded or not, in any form.
Policy	A written statement that communicates management's intent, objectives, requirements, responsibilities, and/or standards.
Preference data	Data about an individual's likes and dislikes.
Privacy	Freedom from unauthorized intrusion.
Privacy commissioner	Independent body that supervises governmental, and eventually private sector, privacy practices.
Privacy impact assessment	An analysis of how information is handled: (i) to ensure handling conforms with applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privacy officer	Internal function responsible for implementing and monitoring an organization's privacy program. Usually, this function is the focal point for external requests, complaints, and supervisory bodies.
Privacy program	The policies, communications, procedures, and controls in place to manage and protect personal information in accordance with applicable laws, regulations, and best practices.
Privacy rights	The legal ability for an individual to take specific actions or make requests with regard to the uses and disclosures of his or her information.
Privacy statement	A document describing an organization's position on privacy, detailing what information it collects, with whom the data is shared, and how users can control the use of their personal data.
Profiling	The use of personal data to create or build a record on a data subject for the purpose of compiling habits or personally identifiable information.
Purpose	The reason why an entity collects personal information.
Redress mechanism	A person, process, or agency to which a data subject can turn for help. A way to make up for loss or damage.
Safe Harbor Agreement	An agreement between the United States and the EU regarding the transfer of personally identifiable information from the EU to the United States. The Safe Harbor Agreement is consistent with Fair Information Practices. Companies that register for Safe Harbor with the U.S. Department of Commerce and abide by the agreement are deemed by the EU to provide adequate data protection for personally identifiable information transferred from the EU to the United States.
Safeguard	A technology, policy, or procedure that counters a threat or protects assets.
Secondary use	Using personal information collected for one purpose for a second, unrelated purpose.
Security	The protection of data from unauthorized access, misuse, or abuse, and destruction or corruption of data.
Security incident	Attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
Self-regulation	Organizations' regulation of the activities of their affiliates.

Sensitive personal information	Personal information that requires an extra level of protection and a higher duty of care (e.g., health or medical history, racial or ethnic origin, political opinions, religious beliefs, trade union membership, financial information, or sexual preference).
Surveillance	Systematic investigation or monitoring of the actions or communications of one or more persons.
System	A system consists of five key principles organized to achieve a specified objective. The five principles are: infrastructure (facilities, equipment, and networks); software (systems, applications, and utilities); people (developers, operators, users, and managers); procedures (automated and manual); and data (transaction streams, files, databases, and tables).
Tagging	Labeling for identification and tracking.
Third party	An entity that is not affiliated with the entity that collects personal information or any affiliated entity not covered by the entity's privacy notice.
Transparency	A standard requiring that the processing of personal information is open and understandable to the individual whose data is being processed; it requires an organization to inform users of what personal information it collects and how the data is used.
Use limitation	The inability for personal data to be disclosed, made available, or otherwise used for purposes other than those specified.
Volunteer	To provide information voluntarily for processing.

7.9 Glossary of Acronyms

ADMA	Australian Direct Marketing Association
ADR	Alternative dispute resolution
AICPA	American Institute of Certified Public Accountants
ANSI	American National Standards Institute
APEC	Asian-Pacific Economic Cooperation
CA	Chartered accountant
CAE	Chief audit executive
CICA	Canadian Institute of Chartered Accountants
CobiT	Control Objectives for Information and related Technology
CoE	Council of Europe
COPPA	Children's Online Privacy Protection Act
COSO	The Committee of Sponsoring Organizations of the Treadway Commission
COTS	Commercial off-the-shelf
CPA	Certified public accountant
CPO	Chief privacy officer
CPSR	Computer Professionals for Social Responsibility
DMA	Direct Marketing Association
EPIC	Electronic Privacy Information Center
ERM	Enterprise risk management
eSAC	Electronic Systems Assurance and Control
ETC	Electronic toll collection
EU	European Union
GAPP	Generally Accepted Privacy Principles
GLBA	Gramm-Leach Bliley Act
GTAG	Global technology audit guide
HIPAA	Health Insurance Portability and Accountability Act
IAPP	International Association of Privacy Professionals
ICC	International Chamber of Commerce
IDs	Identifiers
IEC	International Electrotechnical Commission
IFAC	International Federation of Accountants
IIA	Institute of Internal Auditors
ISACA	Information Systems Audit and Control Association
ISAE	International Standards on Assurance Engagements
ISO	International Standardization Organization
ISTPA	International Security Trust and Privacy Alliance
IT	Information technology
ITGI	IT Governance Institute

LAN	Local area network
NTIA	National Telecommunications and Information Administration
OECD	Organisation for Economic Co-operation and Development
OPA	Online Privacy Alliance
P3P	Platform for Privacy Preferences
PA	Practice Advisory
PET	Privacy-enhancing technology
PI	Privacy International
PIA	Privacy impact assessment
PII	Personally identifiable information
PIPEDA	Personal Information Protection and Electronic Documents Act
UN	United Nations
W3C	World Wide Web Consortium

7.10 Authors, Contributors, and Reviewers

About the Authors

Ulrich Hahn, Ph.D., CIA, CISA, CCSA, Independent Trainer and Consultant, Switzerland/Germany

Hahn, who received an advanced Industrial Engineering (Telecommunications) degree from the Technical University of Darmstadt (Germany), initially joined a global accountancy to work on large consulting and assurance assignments for public- and private-sector clients. He then held an audit position with a major financial services data center, and subsequently joined a Big Five IS audit practice. He then worked in corporate audit management functions of global market leaders. Hahn holds a Ph.D. on the development of international data privacy law and is IIA accredited in quality assessment/validation. He is also winner of a William S. Smith Gold Medal Award for achieving the highest score on all parts of the CIA exam in one sitting. He has been European Confederation of Institutes of Internal Auditing chairman, ISACA Germany vice president, IIA-Germany board member, and is currently a member of the IIA International Advanced Technology Committee. He participates in various chapter committees and working groups that focus on professional practices, quality, events, and publications. Hahn writes, speaks, and lectures on information systems and general audit matters, and provides managerial as well as technical support to audit functions within an international network of well-known senior audit professionals. He also teaches CIA, CISA, and CCSA courses in several countries.

Ken Askelson, CIA, CPA, CITP, JCPenney Co., USA

Askelson is senior IT audit manager for JCPenney in Plano, Texas. He supervises the IT audit staff responsible for auditing and monitoring the activities of the IT infrastructure. Previous positions with JCPenney include audit manager, merchandise manager, and regional accounting coordinator. Askelson has served on several committees for the AICPA, including its IT Executive Committee, IT Research Subcommittee, IT Practices Subcommittee, and Business and Industry Executive Committee. He currently serves as a commissioner on the AICPA National Accreditation Commission, vice chair of the AICPA Privacy Task Force, and member of the Editorial Advisory Board for the *Journal of Accounting*. Askelson was a participant in the Partnership for Critical Infrastructure Security sponsored by the U.S. Chamber of Commerce and the Critical Infrastructure Assurance Office of the Department of Homeland Security. In addition, he held various positions with local IIA chapters, currently serves on The IIA's Advanced Technology Committee, and was recognized as "Auditor of the Year" and "Chairperson of the Year" by The IIA's Orange County [California] Chapter. Askelson received degrees in marketing and accounting from the University of Northern Iowa.

Robert Stiles, CISA, CFE, Texas Guaranteed, USA

Stiles is a senior technology auditor at Texas Guaranteed (TG), a not-for-profit, public corporation. He began employment with Texas Guaranteed in 1989, and has held several positions including compliance analyst, investigator, and technology auditor. Stiles' audit activities focus on privacy, security, networks, and Internet applications. He has conducted vulnerability assessments of TG's external network, interior network, and physical security.

Contributors

Sean Ballington, PricewaterhouseCoopers LLP, USA
Nancy Cohen, AICPA, USA
Heriot Prentice, The IIA Inc.
Kyoko Shimizu, PricewaterhouseCoopers, Japan

Reviewers

The IIA Advanced Technology Committee, IIA global affiliates, AICPA, Center for Internet Security, Carnegie-Mellon University Software Engineering Institute, Information Systems Security Association, IT Process Institute, National Association of Corporate Directors, and SANS Institute joined the review process. The IIA thanks the following individuals and organizations who provided comments that added great value to this guide:

- AICPA/CICA Privacy Task Force
- David F. Bentley, Consultant, United Kingdom
- Lily Bi, The IIA Inc.
- Larry Brown, The Options Clearing Corp., USA
- Lars Erik Fjortoft, KPMG, Norway
- Christopher Fox, PricewaterhouseCoopers LLP, USA
- Sara Hettich, Microsoft Corp., USA
- IT Audit Specialty Group, IIA-Norway
- Everett Johnson, Deloitte and Touche (retired)
- Steve Mar, Microsoft Corp., USA
- Stuart McCubbrey, General Motors Corp., USA
- Peter Petrusky, PricewaterhouseCoopers LLP, USA
- Jay R. Taylor, General Motors Corp., USA
- Hajime Yoshitake, Nihon Unisys Ltd., Japan
- Nilesh Zacharias, PricewaterhouseCoopers LLP, USA

Preview of GTAG 6 – Effective Vulnerability Management

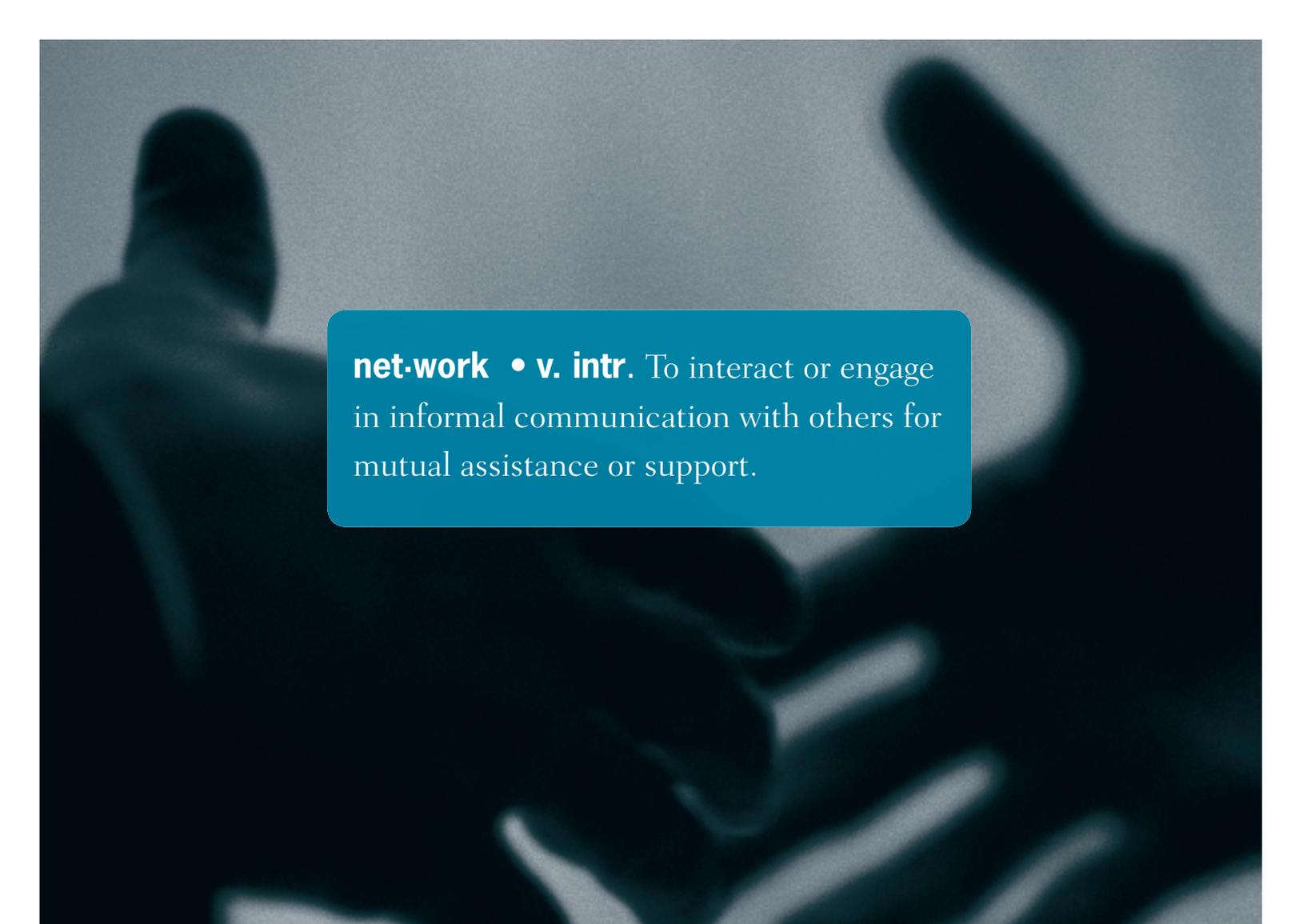
An IT vulnerability is a weakness or exposure in an information system that could lead to a business risk or a security risk. According to the National Vulnerability Database, there are almost 5,000 new vulnerabilities discovered every year and this number has been increasing dramatically each year. Many of them are in high severity and could cause a major disruption within an organization.

Vulnerability management is processes and technologies that an organization employs to identify, assess, and mitigate IT vulnerabilities.

This guide was developed to help Chief Audit Executives to assess the effectiveness of their vulnerability management processes. It recommends specific management practices to guide an organization to achieve and sustain higher levels of effectiveness and efficiency and illustrates the differences between high and low performing vulnerability efforts.

After reading this Guide, you will:

- Have a working knowledge of vulnerability management processes
- Have the ability to differentiate between high and low performing vulnerability management organizations
- Be familiar with the typical progression of capability from a technology-based approach to a risk-based approach
- Provide useful guidance to IT Management on best practices for vulnerability management
- Be able to more effectively sell your recommendations to your CIO, CISO, CEO and/or CFO



net-work • v. intr. To interact or engage in informal communication with others for mutual assistance or support.

THE DEFINITION OF NETWORKING HASN'T CHANGED, BUT HOW WE DO IT HAS.

Introducing Member Exchange – a new online global networking tool!

This free service is available exclusively for members of The Institute of Internal Auditors. This exciting networking tool will allow IIA members to use criteria to search for and connect with colleagues around the globe, and exchange ideas via a technology-based forum.

It's never been easier to network:

1. Visit www.theiia.org/membership and click on Member Exchange.
2. Build your profile by picking the words that best describe your skills and interests as an internal auditor.
3. Pinpoint connections from within your network of IIA colleagues.
4. Start connecting with your global network!

Member Exchange . . . just one more benefit of IIA membership.

www.theiia.org



Progress Through Sharing



PROFESSIONALISM REQUIRES PASSION

To succeed in the work world today, you have to be passionate about your organization, your profession, and your proficiency.

PROFESSIONAL INTERNAL AUDITORS:

- Embrace the *International Standards for the Professional Practice of Internal Auditing* and the Professional Practices Framework.
- Acquire the CIA certification.
- Support quality assurance and improvement programs.
- Pursue continuing education.
- Advocate on behalf of the profession.

Now is your time to shine.

www.theiia.org/Guidance

Managing and Auditing Privacy Risks

One of the many challenging and formidable risk management issues faced by organizations today is protecting the privacy of customers and employees personal information. This GTAG covers privacy concepts, principles and frameworks which will aid Chief Audit Executives, internal auditors, and management to find the right sources as guidance for their organizations. It provides the insight into privacy risks that the organization should address when it collects, uses, retains, or discloses personal information. This GTAG elaborates on how to deal with privacy within the audit process and also provide a generic outline for a privacy audit program.

What is GTAG?

Prepared by The Institute of Internal Auditors, each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology management, control, and security. The GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices. The following guides were published in 2005.

Guide 1: Information Technology Controls

Guide 2: Change and Patch Management Controls: Critical for Organizational Success

Guide 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

Guide 4: Management of IT Auditing

Check The IIA technology Web site at www.theiia.org/technology



**The Institute of
Internal Auditors**

Order Number: 1017

IIA Member US \$25

Nonmember US \$30

IIA Event US \$22.50

ISBN 0-89413-595-3

