Auditing Privacy and Data Protection Risks

3rd Edition

Global Practice Guide

Companion IIA Audit Tools:

- *Privacy and Data Protection RACI Matrix Tool*
- *Privacy and Data Protection RCM Tool*

Aligns with the Global Internal Audit Standards

The Institute of Internal Auditors

GENERAL GUIDANCE

Acknowledgements

Guidance Task Force

Kavin Anburaj, CISA, United States

Farah George Araj, CIA, CRMA, QIAL, FCPA, CFE, Australia

Hassan Khayal, CIA, CRMA, CFE, United Arab Emirates

Brittany Long, CIA, CRMA, CISA, CDPSE, United States

Flaviana Mele, CCSA, Italy

Hyder Ali Mirza, CISA, United Arab Emirates

Thato Moeng, CISA, CISM, South Africa

Maksym Pogorelovskyi, Ukraine

Global Guidance Council Reviewers

Tania Stegemann, CIA, CRMA, CCSA, Australia

Muriel Uzan, CIA, CRMA, Spain

Klaas Jan Westerling, CIA, Netherlands

International Internal Audit Standards Board Reviewers

Michael Levy, CIA, CRMA, United States

James Rose, CIA, CRMA, CPA, CISA, United States

IIA Standards and Guidance

Benito Ybarra, CIA, CFE, CISA, CCEP, Executive Vice President

Katleen Seeuws, CIA, CRMA, CGAP, CFSE, CISA, Vice President

Angela Douglas, CIA, CRMA, Senior Manager, Project Lead

The IIA thanks these volunteers for their invaluable contributions to this guide's previous editions: Ken Askelson, Stefanie Hardgrove, Steve Hunt, Steven Jameson, Sara Lademan, Michael Lynn, and David Williams.

The IIA also thanks the following oversight bodies for their support: Global Guidance Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight Council. To learn more about contributing to Global Guidance, visit https://www.theiia.org/en/about-us/get-involved/volunteer-your-time/.

About the IPPF

International Professional Practices Framework® (IPPF)

A framework provides a structural blueprint and coherent system to facilitate the consistent development, interpretation, and application of a body of knowledge useful to a discipline or profession. The International Professional Practices Framework® (IPPF®) organizes the authoritative body of knowledge, promulgated by The Institute of Internal Auditors, for the professional practice of internal auditing. The IPPF includes Global Internal Audit Standards™, Topical Requirements, and Global Guidance.

The IPPF addresses current internal audit practices while enabling practitioners and stakeholders globally to be flexible and responsive to the ongoing needs for high-quality internal auditing in diverse environments and organizations of different purposes, sizes, and structures.

Global Guidance

Global Guidance supports the Standards by providing nonmandatory information, advice, and best practices for performing internal audit services. It is endorsed by The IIA through formal review and approval processes.

Global Guidance provides detailed approaches, step-by-step processes, and examples on subjects including:

- Assurance and advisory services.
- Engagement planning, performance, and communication.
- Financial services.
- Fraud and other pervasive risks.
- Strategy and management of the internal audit function.
- Public sector.
- Sustainability.

Global Technology Audit Guides® (GTAG®) provide auditors with the knowledge to perform assurance and advisory services related to an organization's information technology and information security risks and controls.

Global Guidance is a benefit of IIA membership.

Contents

Executive Summary

Safeguarding personal data remains one of the most complex and high-stakes challenges in organizational risk management. Personal data is defined as any information that identifies, or can reasonably be used to identify, a living individual or natural person, either directly or indirectly. Individuals, whether customers, employees, governments, stakeholders, or business partners, expect transparency, accountability, and control over how their personal data is collected, used, and shared. Organizations must not only meet these expectations but also uphold contractual obligations and comply with an increasingly intricate web of global privacy, data protection, artificial intelligence (AI), and cybersecurity regulations.

The digital ecosystem continues to evolve rapidly. Organizations are adopting AI, outsourcing data-intensive operations, and deploying internet of things (IoT) devices, all of which amplify privacy risks. High-profile data breaches and regulatory fines have heightened scrutiny from boards and governing bodies, who now demand robust assurance that privacy risks are being proactively managed.

Internal auditors play a critical role in providing this assurance by independently evaluating whether privacy and data protection risks are identified, assessed, and managed across the data lifecycle. This Global Practice Guide:

- Provides an overview of the internal audit function's responsibilities related to auditing privacy and data protection risks.
- Helps internal auditors plan and execute privacy and data protection engagements more effectively by offering practical guidance on governance, scoping, risk assessment, control evaluation, and reporting.
- Equips internal audit functions with a structured methodology, working knowledge of key privacy frameworks, and concrete examples of audit procedures that can be tailored to different industries, technologies, and risk profiles.

This guide supersedes "Auditing Privacy Risks, 2nd Edition," published in 2012. Additionally, two companion tools are offered: Privacy and Data Protection RACI Matrix tool and Privacy and Data Protection RCM tool.

Introduction

Privacy has become a defining issue for organizations in every sector. Massive growth in data processing, cloud computing, advanced analytics, and AI has created new opportunities for innovation, but it has also magnified the consequences of misuse, mishandling, or loss of personal data. **Stakeholders** increasingly judge organizations not only on what they deliver, but also on how responsibly they treat the personal data entrusted to them.

Regulators worldwide have responded by strengthening privacy and data protection laws, imposing stricter obligations on organizations and establishing significant penalties for noncompliance. Individuals have also gained broader rights to understand and influence how their data is processed. As a result, privacy and data protection **risks** now span legal, operational, financial, and reputational dimensions and deserve focused attention in the enterprise **risk management** framework.

Note

Terms appearing in **bold blue** are defined in the Global Internal Audit Standards. To understand and implement the Standards correctly, it is necessary to understand and adopt the specific meanings and usage of the terms as described in the glossary.

The Standards use the word "must" in the Requirements sections and the words "should" and "may" to specify common and preferred practices in the Considerations for Implementation sections.

Within this context, **internal audit functions** are expected to provide an independent and objective assessment of whether privacy and data protection risks are being effectively managed. Internal auditors must understand how personal data flows through systems and processes, what controls are in place to protect it, and whether those controls operate effectively in practice. They must also evaluate whether **governance** structures, policies, and accountability mechanisms support a culture of responsible personal data use. Standard 3.1 Competency states, "Internal auditors must possess or obtain the competencies to perform their responsibilities successfully."

This guide introduces a practical methodology for auditing privacy and data protection risks. It summarizes key global privacy frameworks, outlines governance and risk management expectations, and describes a phased approach to planning, executing, and reporting on privacy and data protection **engagements**. It is designed to be adaptable: internal auditors can use it to support dedicated privacy and data protection engagements or integrate privacy and data protection testing into broader engagements such as IT, cybersecurity, or compliance engagements.

What Is Privacy and Why It Matters

Privacy, in the context of organizational risk management, refers to the rights and expectations of individuals regarding the collection, use, sharing, and retention of their personal data. Personal data or personally identifiable information (PII), referred to as personal information in some jurisdictions, typically includes any information that can identify an individual directly or indirectly, such as names, contact details, identification numbers, financial information, location data, or online identifiers. Some laws distinguish between regular personal data and sensitive data, such as health information, biometric data, or information about children, which usually requires additional protections. Refer to Appendix B for examples of personal and sensitive information. In addition to personal and sensitive data, classified data must also be protected.

Privacy is closely related to, but distinct from, information security. While security focuses on protecting the confidentiality, integrity, and availability of information, privacy focuses on whether the organization is doing the right things with personal data in the first place. A system may be technically secure but may still pose privacy risks if the organization collects more data than necessary, uses data for undisclosed purposes, retains it longer than needed, or shares it inappropriately with third parties.

Effective privacy management benefits organizations in multiple ways. It reduces the **likelihood** of regulatory sanctions and litigation arising from noncompliance with privacy and data protection laws and contractual obligations. It strengthens the trust of stakeholders, such as customers and employees, which can directly influence brand perception, customer loyalty, and the ability to attract and retain talent. It also enables responsible innovation by providing clear guardrails for the design and deployment of new data-intensive products, services, and technologies.

Conversely, poor privacy practices can have immediate and long-lasting consequences. Personal data breaches may result in regulatory investigations, fines, class-action lawsuits, costly remediation efforts, and reputational damage. Even when no breach occurs, unclear or unethical data practices can trigger public backlash, social media campaigns, and customer attrition as individuals migrate to competitors they perceive as more trustworthy. In some jurisdictions, senior leaders and **boards** face explicit accountability obligations for overseeing privacy and data protection risk and may be held personally responsible for failures.

For internal auditors, understanding the broader importance of privacy is essential to framing **engagement objectives** and communicating results. Internal audit reports that connect privacy and data protection control gaps to strategic, operational, and reputational **impacts** are more likely to resonate with executive leadership and boards. Focusing on areas where privacy failures would be most consequential for the organization and its stakeholders helps internal audit functions prioritize their limited resources.

Global and Emerging Privacy and Data Protection Frameworks

Internal auditors do not need to be privacy lawyers, but they should understand the content of major privacy frameworks that drive regulatory expectations and control requirements. Although terminology varies, these frameworks share common themes: data minimization, lawful and transparent processing, respect for individual rights, accountability for outcomes, and appropriate technical and organizational safeguards. The following is a high-level overview of selected frameworks that frequently affect multinational organizations.

European Union General Data Protection Regulation (GDPR)

The GDPR is one of the most influential privacy regulations globally. It applies to organizations established in the European Economic Area (EEA) and to organizations outside the EEA that offer goods or services to individuals in the EEA or monitor their behavior. The GDPR emphasizes lawful bases for processing, explicit consent in certain circumstances, robust data subject rights, privacy by design and by default, records of processing activities, and obligations to implement appropriate technical and organizational measures. In many cases, the GDPR requires the appointment of a data protection officer (DPO). In addition, the GDPR requires notification of certain personal data breaches to supervisory authorities and, in some cases, affected individuals within defined timelines.

California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

In the United States, California's state-level privacy laws, or similar laws, have been adopted in other parts of the country. An example is the Connecticut Consumer Data Privacy Act. The CPRA amends and expands the CCPA, granting California residents rights such as knowing what personal data is collected, accessing and correcting that data, opting out of certain data sales and sharing, and limiting the use of sensitive personal data. The CPRA established the California Privacy Protection Agency to enhance enforcement capabilities and introduce new obligations related to data minimization, retention, and **risk assessments** for certain high-risk processing activities.

In addition to these frameworks, jurisdictions across the globe, such as Australia and China, also have frameworks. Internal auditors should consult the local legislation and industry-specific best practices of their specific jurisdiction.

Refer to Appendix A for additional global and emerging privacy and data frameworks.

Governance, Roles, and Accountability

Strong governance is the foundation of effective privacy and data protection risk management. Governance establishes how decisions about personal data are made, who is responsible for them, and how performance is monitored and reported. Internal auditors should expect to see privacy and data protection integrated into an organization's overall governance, risk management, **control processes**, and compliance framework.

Boards typically oversee privacy and data protection as part of their broader risk oversight responsibilities. They should receive periodic reporting on privacy and data protection risks, regulatory developments, significant incidents, and the effectiveness of management's response. **Senior management** is responsible for establishing a privacy and data protection strategy, assigning roles, approving policies, and ensuring that sufficient resources and expertise are available to manage privacy and data protection risks.

Many organizations designate a data protection officer or an equivalent privacy leader, which may be required by law in certain jurisdictions or voluntarily established as a best practice. The DPO or privacy office typically coordinates privacy policies, advises on compliance obligations, oversees data protection impact assessments, manages data subject rights requests, and acts as a liaison with regulators.

Operational accountability for privacy and data protection is distributed across business units such as IT, security, HR, compliance, procurement, marketing, and other functions that collect or use personal data. One of this Global Practice Guide's companion tools, Privacy and Data Protection RACI (Responsible, Accountable, Consulted, Informed) Matrix, can help clarify who is responsible for which aspects of privacy and data protection, such as data classification, access approvals, vendor due diligence, consent management, and incident response. Training and awareness programs reinforce these responsibilities and promote a culture in which employees understand and respect privacy and data protection obligations.

While internal auditing should not own or manage privacy or data protection risks, it plays an essential role in independently assessing whether governance structures function as designed, whether roles and accountabilities are clear and effective, and whether the first and second lines are adequately managing privacy and data protection risks. If internal auditors determine that privacy and data protection risks are not adequately managed, they must determine whether to develop recommendations, request action plans from management, or collaborate with management to agree on actions that align with the organization's **risk appetite** and strategic objectives (Standard 14.4 Recommendations and Action Plans).

Privacy and data protection governance should provide clear escalation paths for ethical concerns related to personal data use, particularly where proposed practices fall within legal boundaries but may exceed the organization's stated risk appetite or ethical commitments.

Risk Assessment and Management of Privacy Risks

Effective privacy and data protection risk management begins with understanding how personal data flows through an organization's ecosystem. According to Standard 13.2 Engagement Risk Assessment, "Internal auditors must develop an understanding of the **activity under review** to assess the relevant risks." Data-mapping or records of processing activities help document what personal data is collected, why it is processed, where it is stored, who has access to it, with whom it is shared, and for how long it is retained. This understanding enables management to identify risk scenarios, assess inherent risk levels, and prioritize control activities. This guide's other companion tool, Privacy and Data Protection RCM (Risk and Control Matrix, includes suggested baseline risks and controls that internal audit functions can revise to fit their industry, **risk tolerance**, and organization.

Common privacy and data protection risk scenarios include:

- Unauthorized access to personal data.
- Lack of privacy obligation awareness across the organization.
- Misuse of data for purposes beyond those disclosed.
- Inadequate consent or transparency mechanisms.
- Excessive data collection or retention.
- Inaccurate or incomplete data.
- Inadequate response to data subject rights requests.
- Noncompliance with cross-border transfer restrictions.
- Insufficient data breach response.

Technology changes, mergers and acquisitions, new products, vendor relationships, and regulatory updates can all introduce new privacy and data protection risks or change the profile of existing risks.

Organizations should incorporate privacy and data protection considerations into their enterprise risk management (ERM) processes. This typically involves defining a risk taxonomy that includes privacy and data protection risks, establishing risk appetite and tolerance levels, and using a consistent methodology to evaluate likelihood and impact. Privacy impact assessments (PIAs) and data protection impact assessments (DPIAs) provide structured approaches to evaluating high-risk processing activities, such as large-scale profiling, use of sensitive data, or deployment of new AI-driven capabilities.

Risk treatment strategies may include implementing or enhancing controls, modifying processes, reducing the scope of data collected, anonymizing or pseudonymizing data, renegotiating third-party contracts, or, in some cases, discontinuing certain activities altogether. Management should track privacy and data protection risks and mitigation actions in risk registers or similar tools, assign owners, and monitor progress. Metrics and key risk indicators, such as volume of data subject requests, frequency of privacy incidents, completion of training, or results of control testing, can help leadership understand trends and adjust priorities.

To strengthen governance and oversight, organizations should explicitly align privacy and data protection risk appetite with board-approved enterprise risk management statements. Privacy risk appetite should articulate the level and types of privacy and data protection risks the organization is willing to accept in pursuit of its strategic objectives, considering regulatory obligations, stakeholder expectations, and ethical considerations.

Board-approved ERM frameworks should incorporate privacy and data protection as a distinct risk category or clearly embedded component within legal, compliance, technology, or reputational risk categories. This alignment enables consistent risk evaluation, prioritization, and reporting across the organization and supports informed decision-making at the board and senior management levels.

Internal auditors should assess whether privacy risk appetite statements are formally approved by the board (or a delegated committee), communicated to relevant stakeholders, and operationalized through policies, standards, and risk assessment **methodologies**. Internal auditors should also evaluate whether reported privacy and data protection risks, incidents, and control issues are assessed and escalated in a manner consistent with the organization's stated risk appetite and tolerance levels.

Internal auditors should evaluate not only the existence of risk assessment processes but also their quality and effectiveness. Internal auditors can review data maps, DPIAs, risk registers, and governance meeting minutes to determine whether privacy and data protection risks are identified comprehensively, reassessed **periodically**, and considered in strategic and operational decisions. They can also assess whether the organization's risk appetite for privacy and data protection is clearly articulated and whether actual practices align with that appetite.

Privacy Controls: Organizational and Technical

Privacy controls encompass a broad set of organizational and technical measures designed to reduce privacy and data protection risks. A mature privacy program integrates these controls into the full data lifecycle — from collection and processing to storage, sharing, and deletion. Internal auditors should evaluate both the design and operating effectiveness of controls and consider how they work together as a system rather than in isolation.

Organizational controls often include policies, standards, procedures, and technologies governing how personal data is handled. Examples include data classification and handling standards, acceptable use policies, consent and notice templates, records of processing procedures, and retention schedules. Training and awareness programs ensure that employees understand these policies and know how to apply them in daily activities. Governance committees and approval workflows provide oversight for high-risk processing activities, new technologies, and third-party engagements.

IIA Resources

The IIA's Topical Requirements on Cybersecurity, Third-Party, Organizational Behavior, and Organizational Resilience each support internal auditors performing engagements in specific risk areas outlined in this section. Internal auditors must apply Topical Requirements in conformance with the Global Internal Audit Standards when providing assurance services on that topic.

The IIA's Global Technology Audit Guides "Auditing Identity and Access Management" and "Continuous Auditing and Monitoring" are also helpful resources.

Technical controls provide the mechanisms to enforce privacy and data protection requirements in systems and applications. Access controls and authentication mechanisms restrict access to personal data based on need-to-know and least privilege principles. Encryption protects data at rest and in transit. Logging and monitoring tools help detect inappropriate access or unusual behavior. Data loss prevention technologies, tokenization, and pseudonymization techniques can reduce exposure when data is processed or shared.

Privacy by design and by default means that privacy considerations are embedded into systems and processes from the outset, rather than retrofitted after deployment. This may include collecting only the minimum personal data necessary for a given purpose, offering privacy-friendly default settings, segregating duties to avoid concentration of access, and conducting design reviews that explicitly consider privacy requirements. Internal auditors should look for

evidence that privacy is considered in project methodologies, change management processes, and system development life cycles, and confirm that privacy impact assessments have been performed.

Control over third parties is especially important because many organizations rely on vendors, cloud providers, and other partners to process personal data. Key control elements include due diligence procedures that evaluate vendors' privacy and security practices, standard contractual clauses that specify privacy obligations (such as data processing agreements) and that grant the right to audit, ongoing monitoring of vendor performance, and processes for managing sub-processors. Internal auditors should assess whether third-party controls are proportionate to the sensitivity and volume of personal data involved.

Finally, effective incident management and breach response capabilities are critical components of a control environment. Organizations should have documented procedures for identifying, triaging, investigating, and remediating privacy incidents, as well as for determining whether an incident constitutes a reportable breach under applicable laws or contracts. Regular testing of incident response plans, including tabletop exercises, helps to ensure that the organization can respond quickly and effectively when incidents occur.

Methodology and Phases

The internal auditing approach to privacy should align with the organization's overall audit methodology while addressing the unique characteristics of privacy and data protection risks. The phases of planning and scoping, fieldwork and testing, and evaluation and reporting provide a structured way to design and execute privacy and data protection engagements. Internal auditors can tailor the depth and focus of each phase based on the organization's size, risk profile, and regulatory environment.

Planning and Scoping

Effective planning is essential to a successful privacy and data protection engagement. During this phase, the internal audit function clarifies objectives, determines the scope, and aligns expectations with stakeholders (Standard 13.3 Engagement Objectives and Scope). Typical engagement objectives include assessing the adequacy of privacy governance and risk management, evaluating the design and operating effectiveness of key controls, and determining whether privacy and data protection practices comply with applicable laws, regulations, and internal policies.

Scoping decisions should be risk-based. Internal auditors may focus on particular business units, geographic regions, systems, data warehouses, data categories, or high-risk processing activities. For example, an engagement may concentrate on a customer analytics platform that uses profiling, a shared services center processing payroll data, or a cloud-based customer relationship management system that supports multiple regions. When defining the scope, internal auditors should consider factors such as data sensitivity, processing volume, regulatory exposure, recent incidents, and upcoming strategic initiatives.

During planning, internal auditors should perform preliminary research, including reviewing relevant laws and regulations, internal policies and standards, prior audit reports, regulatory **findings**, and risk assessments. They should also meet with key stakeholders, such as the data protection officer or privacy office, IT and security leaders, process owners, and legal/compliance counsel, to understand current privacy initiatives and challenges. This helps ensure that the engagement focuses on areas of greatest concern and avoids duplicating other **assurance** activities (Standard 9.5 Coordination and Reliance and the Global Practice Guide "Coordination and Reliance: Working with Other Assurance Providers").

The planning phase culminates in an **engagement work program** that defines engagement procedures, sampling approaches, and timelines (Standard 13.6 Work Program). It should also address logistical considerations, such as access to systems and data, coordination with other assurance providers, and the handling of any highly sensitive information that the internal audit function may need to review (Standards 5.1 Use of Information and 5.2 Protection of

Information). Where privacy laws restrict access to certain data, internal auditors may need to work with anonymized or synthetic data or rely on system configuration evidence instead of direct data inspection.

Fieldwork and Testing

Fieldwork involves executing the engagement procedures defined during planning and gathering relevant, reliable, and sufficient evidence to support **engagement conclusions** (Standard 14.1 Gathering Information for Analyses and Evaluation). As privacy and data protection are cross-functional, fieldwork often requires collaboration with multiple stakeholders and may involve both process-level and technical testing. Internal auditors must document their procedures and results in accordance with internal auditing standards and methodologies (Standards 4.1 Conformance with the Global Internal Audit Standards and 9.3 Methodologies).

Typical fieldwork activities include interviewing process owners to understand how personal data is collected, processed, shared, stored, or retained; reviewing policies, procedures, and training materials; and examining documentation such as data inventories, data protection impact assessments, data management processes, records of processing activities, and vendor contracts (Standard 14.1). Internal auditors may also perform walkthroughs of key processes, such as onboarding of new customers or employees, handling data subject access requests, classification of systems with higher privacy risk (particularly those that also use AI functionalities), or provisioning and deprovisioning user access to systems containing personal data.

Testing may involve reviewing system configurations (including conducting vulnerability assessments and penetration tests), access control lists, data classification schemas, encryption settings, logging and monitoring tools, data retention or deletion jobs, and physical controls. Internal auditors should categorize hardware into fixed infrastructure (servers, routers, switches) and mobile endpoints (laptops, tablets, and smartphones), as their respective risk profiles differ significantly.

While fixed assets are usually kept in controlled environments, mobile devices create higher privacy risks. These risks include theft during transport and exposure to unsecured public networks. As a result, organizations should assess controls for fixed and mobile assets separately, necessitating a bifurcated approach to control assessments. Vulnerability assessments and penetration tests may be conducted by management or third parties (Standard 9.5). Where appropriate, internal auditors may use data analytics to identify unusual patterns, such as access to sensitive records outside business hours or duplicate uploads of personal data to non-approved repositories.

IIA Resources

The IIA's "Data Analytics Guidance and Resources for Internal Auditors" offers information on skills and competencies needed to understand and use data analytics.

In addition, social engineering, which is the practice of manipulating people into revealing confidential information or performing actions that compromise security, should be tested. Internal auditors should assess social engineering controls and outcomes (such as phishing

simulations, identity verification procedures, and escalation playbooks), and where approved, conduct controlled tests to validate adherence (Standard 14.2 Analyses and Potential Engagement Findings). In all cases, the internal audit function must handle any personal data accessed during testing in a secure and compliant manner, consistent with the organization's own privacy expectations (Standards 5.1 Use of Information and 5.2 Protection of Information).

Sampling is a critical aspect of fieldwork. Internal auditors should design sampling methods that provide reasonable assurance while remaining practical, document their rationale, and clearly distinguish between judgmental and statistical samples in their **workpapers** and reports (Standard 14.6 Engagement Documentation).

Throughout fieldwork, internal auditors should remain alert to indicators of emerging risks or systemic issues. For example, repeated reliance on manual workarounds, inconsistent documentation, or heavy dependence on a few key individuals may signal underlying control weaknesses. When significant issues are identified, internal auditors must discuss them with management as the engagement progresses, allowing for timely corrective actions or clarifications (Standard 13.1 Engagement Communication).

Evaluation and Reporting

In the evaluation phase, the internal audit function synthesizes findings from fieldwork, assesses their **significance**, and forms overall conclusions about the effectiveness of privacy and data protection governance, risk management, and control processes. This involves comparing observed practices against **criteria** derived from laws and regulations, internal policies, recognized frameworks, and the organization's stated risk appetite and strategic objectives (Standard 13.4 Evaluation Criteria).

Internal auditors should group individual observations into themes (Standard 11.3 Communicating Results), such as governance and oversight, risk assessment, data lifecycle management, third-party risk, technical safeguards, or incident response. Internal auditors must collaborate with management to identify the **root causes**, when possible (Standard 14.3 Evaluation of Findings), for example, unclear accountability, insufficient resources, inadequate training, or system limitations, and consider whether issues are isolated or indicative of broader systemic weaknesses.

To determine the significance of a risk, findings must be prioritized based on the likelihood of the risk occurring and the impact the risk may have on governance, risk management, and control processes (Standard 14.3). High-priority issues might include unmitigated legal noncompliance, weak controls over sensitive data, repeated failures to meet breach notification timelines, or significant backlogs in responding to data subject rights requests. As per Standard 14.4 Recommendations and Action Plans, "Internal auditors must determine whether to develop recommendations, request action plans from management, or collaborate with management to agree on actions." If internal auditors and management disagree about the engagement recommendations and/or action plans, internal auditors must follow an established methodology to allow both parties to express their positions and rationale and to determine a resolution (Standard 9.3 Methodologies).

The final engagement communication must present conclusions in an accurate, objective, clear, concise, constructive, complete, and timely manner (Standards 11.2 Effective Communication and 15.1 Final Engagement Communication and the Global Practice Guide "Communicating Final Engagement Results"). Executive summaries should highlight key themes and overall ratings (although not required). Detailed sections can provide context, describe testing performed, and outline specific findings and recommendations (Standard 14.5 Engagement Conclusions). Where appropriate, internal auditors may also include positive observations about effective practices or recent improvements to help reinforce desired behaviors. If a final engagement communication contains a significant error or omission, determined according to criteria agreed upon with the board, the **chief audit executive** must communicate corrected information promptly to all parties who received the original communication (Standard 11.4 Errors and Omissions).

After issuing the final engagement communication, internal auditors should follow up on management action plans to verify that remediation efforts are completed and effective (Standard 15.2 Confirming the Implementation of Recommendations or Action Plans). If management has not progressed in implementing the actions according to the established completion dates, internal auditors must obtain and document an explanation from management and discuss the issue with the chief audit executive. The chief audit executive is responsible for determining whether senior management, by delay or inaction, has accepted a risk that exceeds the risk tolerance (See also Standard 11.5 Communicating the Acceptance of Risks).

Given the dynamic nature of privacy and data protection risks, follow-ups may also involve monitoring regulatory developments and emerging technologies that could affect the relevance of earlier recommendations.

Sector-Specific Applications

While core privacy and data protection principles are broadly applicable, sector-specific regulations, business models, and risk profiles shape how organizations implement privacy and data protection controls. Internal auditors should tailor their procedures to reflect these subtle differences. The following examples highlight how privacy and data protection risks and controls can often manifest in healthcare, financial services, retail, and the public sector.

Healthcare

Healthcare organizations process large volumes of highly sensitive personal data, including medical records, diagnostic information, genetic data, and payment details. Laws such as the United States' Health Insurance Portability and Accountability Act (HIPAA) establish national standards for protecting health information and define specific requirements for covered entities and business associates. Healthcare providers must manage privacy alongside patient safety and clinical effectiveness.

Typical privacy and data protection risks in healthcare include inappropriate access to patient records by staff, unauthorized disclosure of information to third parties, misconfigured electronic health record systems, use of tracking technologies without appropriate consent, and insufficient safeguards when sharing data for research and telehealth. Ransomware and other cyberattacks also pose significant threats to confidentiality and availability.

Internal auditors in healthcare settings may review HIPAA and other jurisdiction-based privacy and security rule compliance, evaluate controls over electronic health record access and monitoring, assess procedures for obtaining and documenting patient authorization, and test the adequacy of breach notification and incident response processes. They should also consider risks associated with third-party service providers, such as billing companies, cloud hosting providers, and telehealth platforms.

Financial Services

Financial institutions manage extensive personal and financial information about customers, counterparties, and employees. In the United States, the Gramm-Leach-Bliley Act (GLBA) imposes privacy and safeguarding obligations on financial institutions, including requirements to provide privacy notices, limit the sharing of certain information, and implement an information security program. Other jurisdictions have similar regimes tailored to their financial sectors. For example, the European Union's Digital Operational Resilience Act (DORA) establishes a harmonized framework requiring financial entities to manage information and communication technology (ICT) risks, report major ICT-related incidents, conduct digital operational resilience testing, and strengthen oversight of ICT third-party providers.

Privacy risks in financial services include misuse of transaction data for undisclosed purposes, insufficient authentication controls leading to account takeover, inadequate monitoring for insider abuse, and noncompliant sharing of customer data with affiliates, fintech partners, or data brokers. The growing use of open banking interfaces and real-time payment systems further increases the importance of strong privacy and data protection practices.

Internal auditors may evaluate GLBA compliance and other jurisdiction-based regulations, review the design and operating effectiveness of customer identity and access management controls, assess data governance for customer and transaction data, and test controls over third-party access to financial data. They should also consider algorithmic decision-making and credit-scoring models, which may introduce bias or transparency concerns alongside privacy implications.

Retail

Retailers routinely collect personal data through loyalty programs, e-commerce platforms, mobile applications, in-store sensors, and targeted advertising campaigns. They may track browsing behavior, purchase histories, location data, and responses to marketing communications. While this data enables personalization and revenue growth, it also raises significant privacy and data protection expectations and regulatory scrutiny, especially when minors and sensitive data types (such as health and financial data) are involved.

Common privacy and data protection risks in retail include nontransparent data collection practices, overbroad or vague privacy notices, sharing of data with advertising networks without appropriate consent or opt-out mechanisms, and weak controls over customer profiles and payment information. Physical stores that use video analytics, Wi-Fi tracking, or other in-store technologies must also consider privacy and data protection implications and, in some jurisdictions, are required to post clear notices about these technologies and obtain customer permission before collecting certain types of data.

Retail-focused privacy and data protection engagements may examine the clarity and accessibility of privacy notices, consent and preference management mechanisms, practices for collecting and storing customer identifiers, the handling of cookies and tracking technologies, and controls over e-commerce platforms and point-of-sale systems. The Payment Card Industry Data Security Standard (PCI DSS), a set of security requirements created by major payment card brands to help organizations protect cardholder data, applies to retailers that store, process, or transmit payment card information and focuses on controls like network security, access management, monitoring, and regular testing to reduce **fraud** and breaches.

Internal auditors should also assess how retailers manage data subject rights requests across online and offline channels.

Public Sector

Public sector entities often process personal data on a broad scale as part of delivering essential services, administering benefits, enforcing laws, and maintaining public records. Individuals may

have limited ability to opt out of such processing, which heightens the responsibility of public bodies to manage privacy and data protection risks carefully and transparently.

Privacy and data protection risks in the public sector may involve large-scale databases of citizen information, identity systems, surveillance technologies, and data sharing between agencies or with private partners. Public sector organizations may also operate legacy systems that present challenges for implementing and maintaining modern privacy and security controls.

Internal auditors in public sector organizations should assess whether privacy considerations are embedded into policy development, program design, and digital transformation initiatives. They can review data-sharing agreements between agencies and levels of government, evaluate controls over access to citizen records, and test the effectiveness of mechanisms for informing individuals about how their data is used and for responding to privacy and data protection complaints or requests.

Emerging Privacy and Data Protection Topics

Privacy risk is not static. New technologies, business models, and regulatory developments continuously reshape the landscape. Internal auditors should stay informed about emerging privacy and data protection topics and consider how to incorporate them into risk assessments and the engagement scope. The following are some areas that may warrant attention.

Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning systems increasingly rely on large volumes of personal and behavioral data to train models and make automated decisions. These systems can create powerful insights but may also introduce new privacy and data protection risks, such as opaque profiling, unintended inference of sensitive attributes, and reuse of data beyond originally specified purposes. Some AI applications, such as facial recognition or emotion analysis, raise heightened ethical and regulatory concerns.

Internal auditors should consider whether AI governance frameworks exist and whether they address privacy and data protection alongside fairness, robustness, and accountability. Key questions include whether training data sets are appropriately sourced and documented, whether data minimization and anonymization techniques are applied where feasible, whether individuals receive meaningful information about automated decision-making that affects them, and whether the organization is relying on third parties. The European Union AI Act and similar initiatives across other jurisdictions highlight that regulators increasingly expect organizations to demonstrate control over AI-related risks.

From an internal audit procedure standpoint, internal auditors may review AI use case inventories, examine documentation of data sources and model training processes, evaluate privacy impact assessments for AI projects, and assess monitoring mechanisms for detecting deviations or unintended outcomes. For technical expertise, internal auditors may collaborate with data scientists, external experts, or the organization's model risk management function.

IIA Resource

The IIA's Global Practice Guide "Auditing Model Risk Management" provides additional information.

Cross-Border Data Transfers

Many organizations operate across borders and routinely transfer personal data between countries for processing, storage, or support. Privacy and data protection laws often impose conditions on such transfers, especially when data moves from jurisdictions with strong protections to those with weaker protections. Mechanisms such as adequacy decisions, standard contractual clauses, binding corporate rules, and sector-specific arrangements are commonly used to legitimize cross-border transfers.

Risks in this area include inadequate documentation of transfer mechanisms, failure to conduct required transfer risk assessments, inconsistent use of contractual clauses, and lack of oversight of onward transfers by third parties or sub-processors. Regulatory decisions and court rulings can change the permitted mechanisms or introduce additional safeguards, making this a dynamic area for compliance.

Internal auditors should review inventories of cross-border data flows, evaluate the use of transfer mechanisms and related due diligence, and assess how legal and regulatory developments are monitored and incorporated into policies and contracts. They may also test controls to ensure that actual data flows align with documented transfer arrangements and that appropriate technical safeguards, such as encryption and key management, complement legal mechanisms.

Data Subject Rights Management

Many privacy laws give individuals specific rights over their personal data. These rights may include the ability to access, correct, delete, or transfer their information, as well as the right to object to certain uses of the data or to withdraw consent. Effective management of data subject rights requests is both a legal requirement and a key indicator of an organization's respect for individual autonomy.

Challenges in managing these requests include verifying the identity of requesters, locating all relevant data across disparate systems and archives, responding within statutory timelines, and balancing privacy and data protection rights with other obligations, such as legal hold requirements or third-party rights. High volumes of requests, particularly following public campaigns or data breaches, can strain resources and expose process weaknesses.

Internal auditors can review policies and procedures for handling data subject rights requests, evaluate the design of request intake channels such as web forms or contact centers, and test samples of completed requests to assess timeliness, completeness, and accuracy. They should also consider whether metrics on request volumes and outcomes are reported to management and used to inform process improvements and resource planning.

Cloud and Third-Party Risks

Cloud services and outsourcing arrangements allow organizations to scale rapidly and access advanced capabilities, but they also concentrate privacy and security risks in third-party environments. Organizations that use cloud storage for protected data should know the physical

location of the storage for data protection regulations. Employee use of AI tools that are not sanctioned by the organization also poses a risk. The shared responsibility model means that the organization, its employees, and its providers have important roles in protecting personal data, and misalignment between assumptions and reality can lead to control gaps.

Risks in this area include inadequate due diligence on providers, overreliance on generic contractual clauses without understanding actual technical controls, misconfigurations of cloud resources, and limited visibility into sub-processors or data residency. Shadow IT, where business units procure cloud services outside central IT oversight, further complicates risk management.

Internal auditors should evaluate the organization's third-party risk management framework, with particular emphasis on employees and providers that process personal data. Internal audit procedures may include reviewing due diligence assessments, contracts and data processing agreements, security and privacy certifications, and monitoring reports; testing configurations in cloud environments; and assessing how findings from engagements or certifications are tracked and addressed.

Breach Notification and Response

Despite robust controls, privacy incidents and data breaches can still occur. When they do, a timely and coordinated response is crucial to limiting harm to individuals, complying with legal and contractual obligations, and maintaining stakeholder trust. Many privacy and data protection laws require organizations to notify regulators and, in some cases, affected individuals, within specific timeframes when certain types of breaches occur.

> **IIA Resource**
>
> The IIA's Global Technology Audit Guide "Auditing Cyber Incident Response and Recovery" provides additional information.

Key elements of an effective breach response capability include clear incident definitions and severity classifications; processes for detecting, triaging, and investigating potential incidents; coordination between IT, security, legal, privacy, communications, and business teams; and mechanisms for documenting decisions and actions taken. Organizations should also maintain contact lists and templates for notifications where required.

Internal auditors can assess breach response readiness by reviewing incident response plans, evaluating lessons learned from prior incidents, and participating in or reviewing results from tabletop exercises. They may also test whether incidents are consistently logged and analyzed, whether root causes are addressed, and whether communication with regulators, customers, and other stakeholders is accurate, timely, and coordinated.

Legal Compliance and Ethical Data Use

Compliance with privacy and data protection laws establishes a minimum baseline for acceptable behavior, but it does not, by itself, ensure ethical data use. Organizations may process personal data in ways that are technically lawful yet inconsistent with stakeholder expectations, societal norms, or the organization's stated values.

Ethical data use considers broader questions such as fairness, proportionality, transparency, and respect for individual autonomy. This includes assessing whether data collection is excessive relative to the stated purpose, whether individuals would reasonably expect a particular use or sharing of their data, and whether automated decision-making or profiling could result in unintended bias or harm, even when legally permissible.

Boards and senior management should, therefore, promote a culture in which decisions about personal data are evaluated not only against legal requirements but also against ethical principles and reputational considerations. Policies, governance forums, and escalation mechanisms should encourage employees to raise concerns about data practices that may be lawful but ethically questionable.

Internal auditors should assess whether governance frameworks and decision-making processes explicitly address this distinction. While internal auditing does not determine lawful purpose or business justification, it can evaluate whether management has established mechanisms to identify, debate, document, and oversee ethical considerations related to personal data use and whether these considerations influence risk assessments, approvals, and controls.

Appendix A. Additional Privacy and Data Protection Frameworks

Here is a sampling of additional privacy and data protection frameworks from global jurisdictions. Internal auditors should consult the local legislation and industry-specific best practices of their specific jurisdiction.

Brazil's Lei Geral de Proteção de Dados (LGPD)

Brazil's LGPD establishes comprehensive rules for personal data processing by public and private entities. It applies beyond the limits of the country's territory when processing involves data subjects located in Brazil, similar to the GDPR's expansive reach. The LGPD sets out lawful bases for processing, data subject rights, transparency obligations, and requirements for data controllers and processors, including the appointment of a data protection officer in many cases. Brazil's National Data Protection Authority (ANPD) issues guidance and can impose sanctions for noncompliance.

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)

Canada regulates privacy through a mix of federal and provincial laws. PIPEDA is Canada's federal private sector privacy law that sets ground rules for how organizations collect, use, and disclose personal information in commercial activities. It is principles-based and includes accountability and consent requirements, is overseen by the Office of the Privacy Commissioner, and can be enforced through investigations, engagements, compliance agreements, and (where pursued) Federal Court remedies.

European Union (EU) Artificial Intelligence (AI) Act

While not a privacy law in the traditional sense, the EU AI Act has major implications for privacy because many AI systems process personal data or infer sensitive attributes. The EU AI Act adopts a risk-based approach, prohibiting certain AI uses, imposing extensive obligations on providers and deployers of high-risk AI systems, and requiring transparency for limited-risk use cases. Internal auditors should be aware that privacy and AI regulatory requirements increasingly intersect, particularly in areas such as automated decision-making, profiling, and biometric identification.

India's Digital Personal Data Protection Act (DPDPA)

India's DPDPA represents a significant evolution in the country's approach to data protection. It establishes principles for lawful processing of digital personal data, recognizes individuals' rights to access, correct, and erase their data in certain circumstances, and sets out obligations for data fiduciaries and processors, including breach notification and security safeguards. The law also contemplates additional responsibilities for significant data fiduciaries based on criteria such as the volume and sensitivity of data processed.

ISO/IEC 27701

ISO/IEC 27701 extends ISO/IEC 27001 to establish a Privacy Information Management System, specifying requirements and guidance for organizations acting as controllers or processors of personally identifiable information. Certifications against these standards can provide a structured framework for security and privacy controls, and internal auditors can leverage them as reference criteria when evaluating the design and effectiveness of control environments.

Japan's Act on the Protection of Personal Information (APPI)

Japan's APPI is the country's principal data protection law and establishes a comprehensive framework for the handling of personal information by businesses and public bodies, with oversight by the Personal Information Protection Commission. It requires organizations to specify the purpose of use for personal information, limit use to that purpose, apply heightened protections to sensitive information, and implement safeguards for personal data, including in connection with third-party disclosures and cross-border data transfers. Amendments that took full effect on April 1, 2022, strengthened individual rights and accountability by expanding rights relating to disclosure, correction, and suspension of use, while also introducing mandatory breach notification in qualifying cases. Internal auditors can use APPI as a reference point when evaluating privacy governance, notice and consent practices, vendor oversight, breach response processes, and controls over international data sharing.

NIST Privacy Framework

The NIST Privacy Framework is a U.S.-based voluntary tool designed to help organizations identify, assess, and manage privacy risk. It uses a similar structure to the NIST Cybersecurity Framework, with core functions such as Identify, Govern, Control, Communicate, and Protect, along with categories and subcategories that organizations can map to their own processes and controls. Internal auditors can use the NIST Privacy Framework to benchmark the maturity of privacy risk management practices and to structure audit procedures around specific outcomes or capabilities.

South Africa's Protection of Personal Information Act (POPIA)

POPIA is South Africa's primary data protection law, implemented to give effect to the constitutional right to privacy by regulating how personal information is collected, stored, and used. It was introduced to align South African business practices with international data security

standards (like the GDPR) and to protect citizens from identity theft and the unauthorized sale of their data. For organizations, the implications of noncompliance are severe, including significant fines, criminal charges, or imprisonment, alongside significant reputational damage. Internal auditors play a critical role in this framework by independently verifying that lawful conditions for processing are met, conducting personal information impact assessments, and ensuring that the organization's internal controls are robust enough to prevent data breaches.

Appendix B. Examples of Personal and Sensitive Information

Type	Examples
Personal Information	• An individual's name, signature, address, phone number, or date and place of birth. • Maiden names or aliases. • Gender. • Marital status. • Email addresses. • Employee record information. • Photographs. • Internet protocol (IP) addresses. • Voice print and facial recognition biometrics.* • Device identification. • Browser history. • Geolocation data from mobile devices.
Sensitive Information	• Racial or ethnic origin. • Political opinions or associations. • Religious or philosophical beliefs. • Trade union membership or associations. • Sexual orientation or practices. • Criminal record. • Health, genetic, or medical information. • Biometric data including fingerprints, retina scans, facial recognition, voice signatures.* • Passwords, PINs, security questions and answers. • Credit card numbers, bank account numbers, tax returns, and financial history. • Social Security numbers or similar identifying data issued by global authorities. • Passport numbers. • Driving license numbers or license IDs. • Information about children.

*** Some countries regard biometric data as personal while others recognize it as sensitive information.**

About The Institute of Internal Auditors

The IIA is an international professional association that serves more than 265,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Volunteer

To learn more about contributing to Global Guidance, visit https://www.theiia.org/end/about-us/get-involved/volunteer-your-time/.

Copyright

May 2026 This version supersedes “Auditing Privacy Risks, 2nd Edition,” published in 2012.

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101