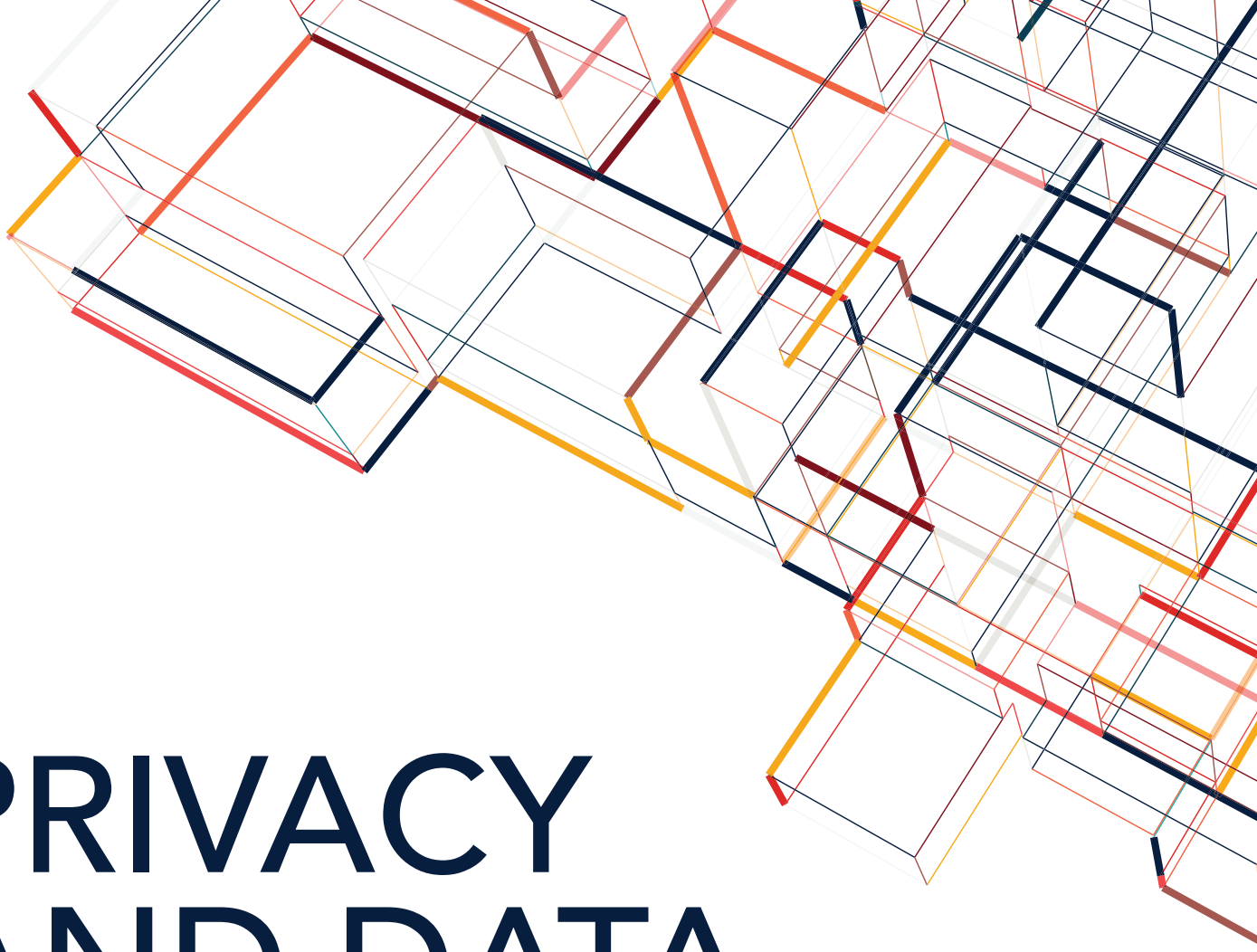


PRIVACY AND DATA PROTECTION

Part 3: Insights Into Effective Collaboration Between Internal Auditors and Data Privacy Professionals

By Adam Pajakowski, CIA, CIPM, CFE, and Kristen Rohrer, CIA, CIPM

Crowe

Internal Audit FOUNDATION

Published by the Internal Audit Foundation
1035 Greenwood Blvd., Suite 401
Lake Mary, Florida 32746, USA

The IIA's International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and the Foundation work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of Foundation-funded research and prepared as a service to the Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or the Foundation.

Table of contents

Introduction and executive summary 4

1) Developing a collaborative approach 7
- Collaboration: A critical factor for growth 7
- The impact of organization size..... 7
- Strategies for better scoping 8
- Internal audit's contribution to privacy thought leadership 9

2) Navigating the regulatory environment.....11
- The evolving privacy landscape 11
- Data mapping: An essential component..... 12
- Cross-border concerns 14
- Risks, roles, and responsibilities..... 15

3) Addressing potential challenges..... 17
- Engaging with senior leadership 17
- Aligning perspectives and objectives..... 19
- Accommodating organizational change..... 20

Conclusion and recommendations..... 22

Internal Audit Foundation 23

Introduction and executive summary

As today's organizations become more reliant on digital technology and collect ever-larger volumes of data, the risks associated with unauthorized access and potential privacy breaches continue to grow. At the same time, the regulatory environment surrounding data protection and privacy is evolving, with governments and standard-setting organizations developing increasingly more comprehensive frameworks to safeguard personal identifiable information.

For internal audit, the impact of these ongoing developments is significant, as understanding and evaluating data protection and privacy risks are critical to internal auditors' responsibility for providing independent, objective assurance and advice on the adequacy and effectiveness of governance and risk management.

Recognizing the importance of navigating this evolving risk landscape, beginning in 2020, the Internal Audit Foundation (the Foundation) and Crowe collaborated on a series of reports. The purpose of these reports is to help internal auditors gain a deeper understanding of privacy and data protection risks and develop a resilient framework to manage them.

Since the launch of the initial report of the series, privacy and data protection have become even more critical risk management concerns. In June 2023, the International Association of Privacy Professionals published the results of interviews and workshops with senior privacy leaders from organizations of various sizes in which 93% of the participants rated privacy as a top 10 organizational risk. Yet, only 64% said they have fully integrated privacy risk management into their overall enterprise risk management programs.[1]

Of even greater concern, only about 21% of the participating organizations reported they had empowered internal audit to undertake privacy audits.[2] This lack of collaboration between privacy professionals and internal audit is particularly striking in view of the high ranking of privacy as an organizational risk.

Moreover, with the rapid advent of generative artificial intelligence and other data-intensive applications, the need for an integrated approach to data protection becomes even more urgent. As a top data security company executive noted in a recent Forbes interview, "The current [software as a service] data infrastructure makes it easier than ever for IT teams to access and share data between companies, regions, and departments."[3] This statement highlights the importance of understanding how conventional organizational policies and procedures will need to adapt to accommodate data infrastructures and tools that increase the accessibility of data across companies, regions, and departments.

The Foundation's own research confirms the need to address associated privacy risks. For example, the findings from the "Risk in Focus 2024" study, published in September 2023, revealed a broad worldwide consensus that cybersecurity – a global, pervasive business risk that has direct implications for data privacy and protection – is a critical consideration when evaluating these programs. In fact, 73% of the 4,207 internal audit leaders surveyed named cybersecurity as the number one area of concern, followed by human capital and business continuity.[4]

Crowe and the Foundation have collaborated on a series of three reports designed to assist internal auditors in assessing their current level of preparedness surrounding privacy and data protection matters.

Privacy and data protection: A three-part series

Part 1: "Internal Audit's Role in Establishing a Resilient Framework." Published in 2020, this report focuses on the history and growth of privacy and data protection issues, including the rapidly expanding regulatory context. Crowe and the Foundation also present an extended discussion of data protection issues and concerns specific to internal audit, as well as outline a general framework for addressing data protection compliance and other risks. The report provides practical steps for the effective implementation of a robust and resilient framework.

Part 2: "Internal Auditors' Views on Risks, Responsibilities, and Opportunities." Published in 2022, this report offers an assessment of the internal audit profession's overall response to data protection and privacy issues, based on an extensive survey of internal audit professionals. In addition to inquiring about their organizations' approaches to data privacy roles and responsibilities, the survey also solicited their views on the materiality of data privacy risk, the effectiveness of their existing privacy policies and practices, and their most critical concerns in this area. The survey findings revealed opportunities for internal auditors to enhance organizational value and assist in identifying, monitoring, and mitigating data privacy risks for their organizations.

---

[1] "Privacy Risk Study 2023" Executive Summary, International Association of Privacy Professionals, June 2023, p. 6, https://iapp.org/media/pdf/resource_center/privacy_risk_study_2023_executive_summary.pdf

[2] Ibid.

[3] Gary Drenick, "Data Security & Privacy Trends For 2023," Forbes, Feb. 2, 2023, https://www.forbes.com/sites/garydrenik/2023/02/02/data-security--privacy-trends-for-2023/?sh=3dc35a706462

[4] "Risk in Focus 2024 Survey Results," Global Summary, Internal Audit Foundation, 2023, p. 6, https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/risk-in-focus-survey-results-global-summary-2024.pdf

Part 3: "Insights Into Effective Collaboration Between Internal Auditors and Data Privacy Professionals." This report builds on Parts 1 and 2, providing a more in-depth examination of how internal audit and privacy professionals are addressing the need to safeguard sensitive information and adhere to regulatory requirements.

One important conclusion that emerged from the previous reports is the need to foster effective collaboration between internal audit and privacy professionals. This third installment of the series further explores the various dimensions of collaboration by highlighting the viewpoints of a group of professionals who engaged in a 90-minute roundtable conversation in the second quarter of 2023.

The roundtable participants included privacy and internal audit leaders based in North America and Europe. Most came from organizations that have operations in multiple jurisdictions, including some whose organizations operate in dozens of countries worldwide. The participants represented organizations of varying sizes in diverse industries – from small specialty businesses to large multinational giants with tens of thousands of employees.

In addition to their perspectives on the importance of collaboration between the internal audit and privacy functions, the participants also shared their current practices and recent experiences regarding engagement and integration between the two functions. The roundtable discussion was organized into three subtopics:

- **Developing a collaborative approach.** Participants provided thoughts on current priorities, strategies, practices, and methods for promoting collaboration between privacy professionals and internal auditors.
- **Navigating the regulatory environment.** Participants offered comments regarding the current state of privacy and data protection regulatory scrutiny and emerging trends or developments that internal auditors should be aware of.
- **Addressing potential challenges.** Participants lent observations and experiences in integrating privacy and data protection into internal audit activities, including key challenges and the criticality of awareness.

These three subtopics provide the basis for the overall structure of the report that follows.

1) Developing a collaborative approach

Regardless of their backgrounds or current perspectives, all participants in the joint Internal Audit Foundation-Crowe roundtable discussion agreed on one critical point: Collaboration between internal audit and privacy professionals is crucial for building robust privacy programs.

Collaboration: A critical factor for growth

The conversation began with one of the participating privacy leaders pointing out the importance of privacy and data security professionals engaging with internal auditors to seek their input in implementing controls, conducting data inventories, and managing policies and procedures related to privacy and security.

"I want to make sure [internal auditors] are involved in the process of building the privacy program, whether it be something very specific … such as [compliance with specific regulatory requirements] or if it's general privacy controls," he said, adding that mutual engagement and communication between parties are vital for growth.

"If we're not talking, then we're not growing," he said.

While consensus among the roundtable participants emphasized the critical role of communication for growth, the participants noted that the level of this collaboration varies greatly, depending on several factors. Among these variables, the size of the organization was one of the most significant considerations.

The impact of organization size

A privacy leader who agreed with the importance of collaboration between the internal audit and privacy functions made an additional observation. Drawing on both her prior experience in very large global corporations and her current position as data privacy officer in a smaller organization, she emphasized that the collaborative efforts observed in her current organization have led to a reduction in knowledge gaps.

"There is a big difference in terms of what I see working for a really large corporation and a small company," she said. "The engagement is very different."

She went on to explain that, at the smaller company, the internal auditor and security and privacy professionals view privacy and security as if they were a product. This internal alignment serves as a strength, helping to create a unified front in addressing privacy concerns.

Another privacy officer from a Fortune 500 corporation offered an additional perspective, explaining how her company addresses the need for collaboration while still maintaining the necessary independence of the two functions.

"We are a large organization and internal audit is intentionally separate from everything else," she said. "We collaborate … and [the internal auditors] are critically important in helping identify, during their audits around the entire enterprise, where they discover personal information being stored or processed."

She noted, however, that the relationship is inherently complicated.

"They also audit us," she said. "So, we have to ensure that we are not basically making them ineffective by creating [an environment that implies that] 'these are the rules by which you can audit us.' So, while we are separate, we do collaborate. They help us [and] we help them, but we maintain our separate purpose."

Nevertheless, she noted, although the foundation, governance, and management of internal audit need to be separate from the business and its operations, collaborating and including internal audit in key areas such as privacy operations has many benefits, and it can be accomplished without compromising internal audit's necessary independence. Moreover, the collaboration goes both ways.

She explained that the privacy office willingly offers its expertise and assistance to internal audit when needed to support a thorough evaluation of privacy-related matters, recognizing that internal auditors might not be privacy specialists.

"Because [internal auditors] are not privacy experts, when they need assistance from the privacy office, in whatever they're going to look at, we can do that," she noted. This type of collaboration allows both teams to effectively address privacy concerns and support the organization's overall goals.

Strategies for better scoping

Another data privacy officer pointed out that, from a data protection and privacy perspective, one significant challenge auditors face is scoping an audit appropriately.

"I know auditors want to see everything but sometimes it's [difficult] to scope [the audit] to what's relevant," she commented, adding that it is crucial to accurately define and understand the different types of data involved. This challenge is especially true for situations in which defining the concept of data and comprehending the various data types can be complex tasks.

"When you talk about data, you can go boil the ocean," she said. "There is IP-type data, there is metadata, there is actual identifiable data, and there is pseudonymized data. … When they go to the audit and when it's scoped, it's useful for internal auditors to know exactly what type of data we're going to audit."

Without such clear definitions and scoping, she added, "I could see a lot of miscommunications, a lot of bad audit results, just because they're misaligned."

From an internal audit perspective, appropriate scoping decisions require an adequate understanding of the types of data and the current regulatory and data privacy environment – in other words, determining which privacy regulations actually apply to the organization. One of the participating internal audit professionals, whose organization operates in numerous countries worldwide, noted that his audit team addresses this issue by collaborating closely with the company's legal team.

"In terms of frequency, we don't have a formal meeting, but any time there's a need to discuss a data privacy-related topic, we get together," he said.

Internal audit's contribution to privacy thought leadership

For one audit professional, the reliance on video meetings during the COVID-19 pandemic demonstrated the growing importance of data protection even in businesses that otherwise might not be considered particularly sensitive to privacy issues. Looking ahead, he proposed the idea of collaborative sessions with the data privacy officer to make auditors more aware of privacy considerations, potential breaches, and the benefits of working with the legal team for compliance training and integrating data privacy discussions into the internal audit process.

"Every time we're collecting data or we're seeing data being exposed or stored somewhere … these are breaches [in which] we help the data privacy officer," he said. "But I think there should also be … sessions with the data privacy officer to make us aware – when we are going to do our audit – what's going to be a breach and then report back. That's the sort of collaboration I can see going forward."

An internal audit leader in the manufacturing sector highlighted the role internal audit can play in helping to elevate the importance of privacy within the organization.

"I see for internal audit there is a chance to contribute toward thought leadership," he said. "If you're a very mature company, you can go and audit it. But before you get there, I think as … professionals that have extensive knowledge, we can help the company get there … [and gradually raise] the importance of privacy and why it needs attention sooner versus later."

"That's a role that I've played," he added. "It took me a couple of years to get there and get everyone on board, but that's building relationships and also being practical."

Rather than limiting his department's role to issuing an audit report that points out risk exposure to the audit committee, this audit leader advocates taking a more solution-oriented approach that asks, "What can we do to incrementally minimize the risk?"

He also explained how internal auditors' experience, connections, and informal interviews with individuals can be useful in gathering stakeholder inputs and identifying potential privacy risks.

"As internal auditors, we know a lot of things across the company, and it could be as simple as what type of information is stored on the shared drive and what third parties have access to our data," he said, recalling a project that brought issues to the table and spelled out a road map for addressing them.

He recounted a successful strategy for gradually elevating the significance of privacy within the organization while still acknowledging the presence of numerous competing priorities. By presenting a constructive road map to the audit committee, he effectively garnered support and collaboration from stakeholders, ultimately propelling the organization's privacy program forward.

"I think everyone was on board and it was really a good project," he concluded. "Lots of hard work and collaboration over several months."

> "Because [internal auditors] are not privacy experts, when they need assistance from the privacy office, in whatever they're going to look at, we can do that.
>
> *– Data privacy leader*

> "As internal auditors, we know a lot of things across the company, and it could be as simple as what type of information is stored on the shared drive and what third parties have access to our data.
>
> *– Internal audit leader*

> "Data privacy resides in our legal team. We're starting to build that expertise, and somehow through some of the work that we've done, we've kind of pushed the organization to invest in data privacy.
>
> *– Internal audit leader*

2) Navigating the regulatory environment

A recurring theme in almost any discussion of privacy risk and data protection is the ever-changing regulatory environment. The challenge inevitably grows in complexity for organizations that have risk exposure in multiple jurisdictions.

The participants in the joint Internal Audit Foundation-Crowe roundtable discussion noted that organizations of all types need to be prepared to defend their data security and access practices, even as the regulatory landscape continues to evolve. Collaboration between internal audit and the privacy office can help in this effort.

The evolving privacy landscape

One noteworthy trend in the evolution of the regulatory environment is a growing consensus that recognizes privacy as a fundamental human right. In discussing this concept, one of the U.S.-based privacy professionals whose company operates on a global scale observed: "What's old is new. Our European colleagues have long said that privacy is a fundamental human right, which means that personally identifiable data always belongs to the individual, regardless of who might have that data for a period of time."

She noted that this perspective, originally codified by the European Union's General Data Protection Regulation (GDPR), is rapidly gaining traction in the United States as well as in other jurisdictions worldwide. A growing number of U.S. states are passing comprehensive privacy laws, and there are recurring discussions at the national level about passing a federal privacy law.

"As this takes hold, I think there are tremendous implications for the internal audit function," she added, noting that one of those implications is a need for organizations to rethink how and why they acquire, handle, and retain personal data.

She recalled that, as data volumes began growing exponentially over the course of several decades, a prevalent attitude among many organizations was "the more data you have, the more power you have." But today, with the growing recognition that personally identifiable data belongs to the individual, organizations are rethinking that approach.

"All of a sudden, the trend might be to have as little data that is personally identifiable as you can possibly get by with," she said.

Data mapping: An essential component

A privacy officer from a large international manufacturing business agreed with that change in perspective.

“I think that when we look at personal data, we tend to be focused on ‘Are we keeping too much? Are we keeping it for the right amount of time?’” But she noted that asking those questions reveals another need.

“What we were lacking was good data mapping,” she recalled. “In order to answer those questions to internal audit legitimately, I have to know where data is being collected in the numerous applications and services that are provided [and] how it’s being shared across different processing activities.”

She pointed out that the GDPR and other regulatory systems now require that companies be able to respond promptly to Data Subject Access Requests, in which individuals exercise their right to access information about all personal data an organization might be processing about them. Privacy regulations require that individuals be able to exercise that right easily and at reasonable intervals.

“The data map is a huge undertaking,” she said. “Without this mapping, we cannot be confident that we can meet the requirements of GDPR or any of the [other data privacy regulations]. … Without having that data mapping, it’s really difficult.”

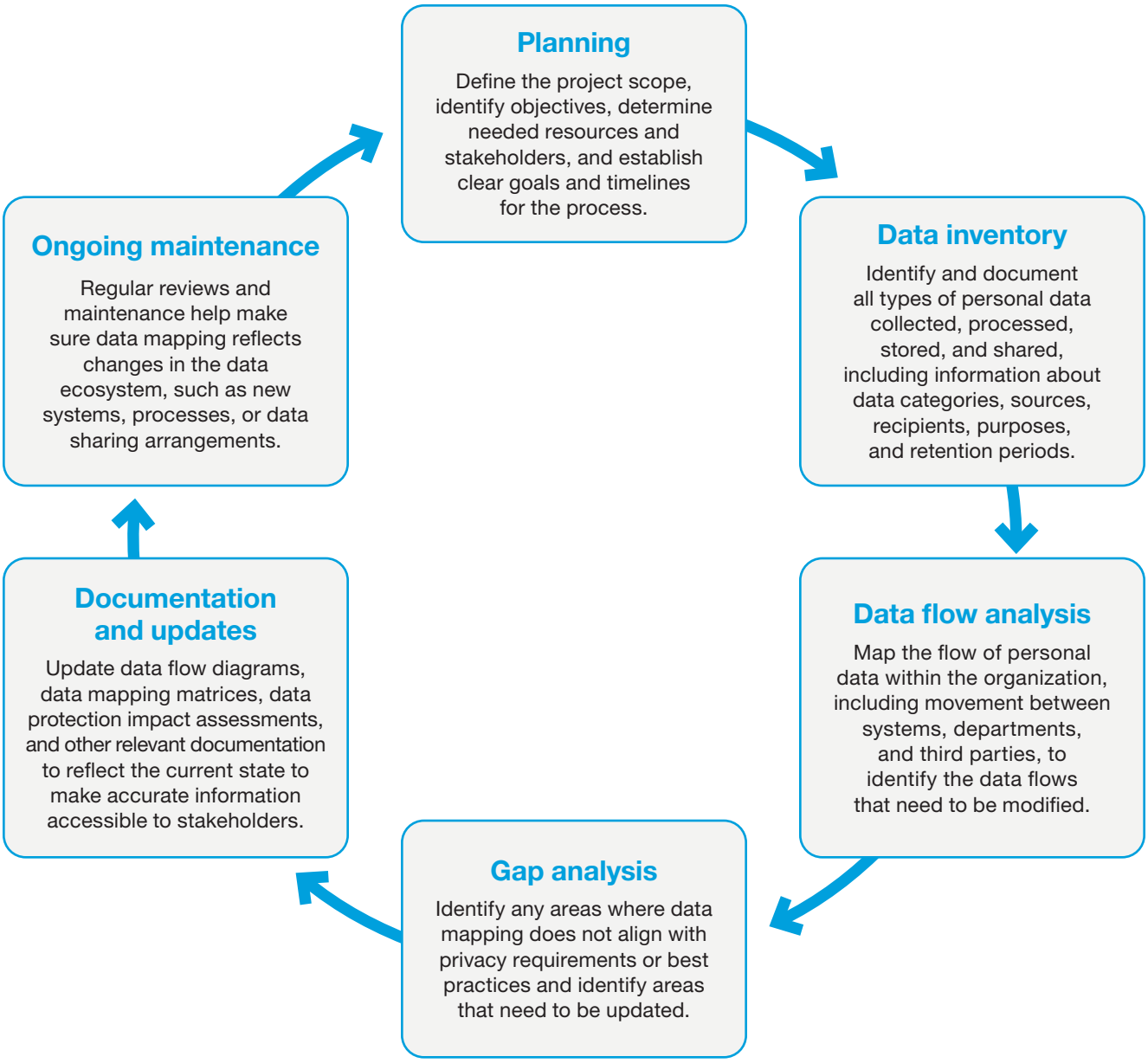
Another privacy professional summed up the issue succinctly: “If you don’t have a data inventory, then you don’t have a privacy program,” he said.

As to the specific implications of these issues on internal audit, one of the participating privacy officers observed: “That’s the emerging trend that’s going to be necessary for auditors to understand when they’re auditing. It isn’t like the old way of auditing, where we are looking at the policies and procedures and identifying those applications that handle [personally identifiable information]. We have to know how it flows [and] where it flows in and out of the organization.”

According to the views of the roundtable participants, having a comprehensive data map helps internal auditors know where to look for specific types of information and better assess the organization’s privacy practices.

Data mapping life cycle

The data mapping process can vary depending on organization size, the data ecosystem's complexity, and the organization's specific needs and requirements. While it is important to tailor the process to each organization, following is a general outline of the typical data mapping life cycle.



Source: Crowe analysis, February 2024

Cross-border concerns

With the rapid growth of global networks, cross-border data transfers present a particular challenge for internal auditors and privacy officers alike.

“A lot of people access data from different locations,” one internal audit professional explained. Because each location in which an employee can access personal data is subject to that location’s unique data privacy regulatory framework, it often is necessary to conduct a third-country risk assessment for each jurisdiction.

Moreover, she added, internal audit must ask specific questions to recognize and evaluate the associated risks.

“What are those controls the company has inside to make sure that the cross-border transfer is properly secured and properly disclosed, and everything is there technically and administratively?” she asked, adding that those questions generally are part of a comprehensive risk assessment in which internal audit seeks answers to additional questions.

“For example, what is the company doing to protect the data from regulatory requests [from other jurisdictions]?” she asked. “Is it in scope? Is it adequate? Is the company prepared to defend the data?”

From her perspective, activities such as assessing measures to safeguard data from regulatory requests in other jurisdictions, evaluating scope and adequacy, and determining the company’s readiness to defend the data are essential components of a comprehensive risk assessment conducted by internal audit.

Risks, roles, and responsibilities

Among the most fundamental of the regulatory issues the participants discussed was the question of who in the organization bears responsibility for staying updated on privacy regulations. One privacy officer noted that in her organization, a Fortune 500 business with global exposure, the privacy office takes the lead in this area.

"Two members of our privacy office are tasked with identifying new privacy regulation requirements," she explained. "They read, keep up on the changes around the world, and they capture and share the details with the top-level management and across the director level."

At the same time, however, other groups – particularly internal audit – also take active roles in monitoring regulatory changes across the company's global operations.

"From an audit perspective, they are looking at similar information because they're not going to wait for [the privacy office] to tell them when they have something new to audit," she said. "So it's everybody's requirement, [even though] the privacy office owns ensuring that applicable privacy training … is created and shared across the enterprise."

While it is reasonable to expect that larger organizations with a dedicated data privacy function will assume ownership, other participants expressed their perspectives on how staying current with the data privacy regulatory environment should be a collective effort.

"I think that, as it relates to privacy requirements, the protection of the data subjects' information, and compliance for the organization, it is [no longer the responsibility of] a single group near the privacy department," said one information security professional. "It is the [responsibility of the] whole organization – and specifically the decision-makers."

Monitoring privacy law

Staying abreast of changing privacy requirements is essential. The following are a few resources that can help organizations stay informed about privacy laws and regulations.

- ✓ **Legislation and regulations**
  A leading and highly influential privacy law is the General Data Protection Regulation. Others include, but are not limited to, Brazil's General Data Protection Law and the China Personal Information Protection Law.

  Data privacy regulations are not uniformly established in every country or U.S. state. In the United States, for instance, although there is no comprehensive federal-level law, certain states have implemented their own privacy regulations, including notable ones like the California Consumer Privacy Act and the California Privacy Rights Act.
- ✓ **Government agencies**
  Government agencies, such as the U.S. Federal Trade Commission or the Information Commissioner's Office in the United Kingdom, often provide guidance and updates on privacy laws.
- ✓ **Industry associations**
  Industry associations, such as the International Association of Privacy Professionals, offer resources, training, and news updates related to privacy laws and regulations.
- ✓ **Legal publications**
  Legal publications, journals, blogs, and newsletters from reputable sources can provide valuable insights into privacy law developments.
- ✓ **Webinars and conferences**
  Participating in webinars and attending conferences focused on privacy law can provide updates, insights, and networking opportunities.

Privacy laws vary by jurisdiction. Many countries have enacted or are in the process of developing privacy regulations. Organizations should monitor sources specific to the regions in which they operate.

He pointed out that privacy and security controls have been well-established for several years, so all decision-makers in an organization should be aware that they can be held directly responsible, both civilly and potentially criminally, for any poor privacy or information security decisions they make that result in harm or a data breach.

Another participant, an internal audit leader in a midsize organization, concurred, adding: "It's kind of a team effort to make sure that nothing falls through the cracks."

He also noted that, despite the progress he believes his organization has made in dealing with privacy risk, there is still more that can be done to mitigate risks.

"One of the things that we're trying to push is also to educate people within the organization to reduce the level of risk when it comes to data privacy," he said. "Everyone has data. … It's like a commodity, and you don't even think about what you have and the potential risk that is involved with handling data. So one of the things that we're trying to do is educate more employees within the organization."

In his view, due to the pervasive nature of data, there is a need to raise awareness about the potential risks associated with handling it.

> "Internal auditors, we desperately need you. I think you can give us such a helpful perspective on how things are really working at the organization.
> *– Data privacy leader*

> "It isn't like the old way of auditing, where we are looking at the policies and procedures and identifying those applications that handle [personally identifiable information]. We have to know how it flows [and] where it flows in and out of the organization.
> *– Data privacy leader*

> "It's kind of a team effort to make sure that nothing falls through the cracks.
> *– Internal audit leader*

> "If you don't have a data inventory, then you don't have a privacy program.
> *– Data privacy leader*

3) Addressing potential challenges

Although there was widespread agreement among participants in the Internal Audit Foundation-Crowe roundtable that collaboration between the internal audit and privacy functions is essential, there was also agreement that integrating privacy and data protection into internal audit activities can pose challenges.

One such challenge is a sense of ownership by all concerned. Like the effort of detecting and preventing fraud, ensuring data privacy should be a collective responsibility for everyone involved.

Data privacy programs share a similarity with anti-fraud efforts in that both require a foundation of a tone from the top. Senior leadership engagement is essential and requires a deliberate outreach effort. The roundtable participants described several initiatives that helped align differing perspectives within their organizations.

Engaging with senior leadership

As with any complex, long-term initiative, the effort to promote effective collaboration among internal audit and privacy professionals requires a strong commitment from the organization's top leadership. The roundtable participants believe both functions can help initiate such commitment by making concerted and coordinated outreach to the highest levels of the organization. This effort aims to increase awareness and engagement with privacy and data protection issues among board and senior executives.

"You have those in internal audit that do talk directly to leadership, directly to the board, and sometimes that is different than where the … privacy professionals go in terms of reporting structure," one of the privacy leaders noted. "But there are times where you put that ad hoc team of privacy professionals together, which includes general counsel, internal audit, the CISO, and a variety of people, and you have a much broader impact on the organization because they each report differently to leadership or to the board."

"And if you can all collaborate with each other … then even though we're each doing our individual jobs, we're going to the same goal," he added. "But because we each report differently to the organization at times, then we can have a much broader support base for those initiatives."

This perspective highlights the extensive impact that a collaborative approach can have on an organization, in which each professional performs individual roles but collectively all contribute to achieving the same goal.

Another participating privacy professional highlighted the need for effective communication, particularly when it comes to engaging with senior leadership.

"What I find interesting is that a lot of times senior leadership [doesn't] really understand what privacy is and what the risks are," she said. "Then when privacy professionals try to explain, they use different language and sometimes that language does not register with senior leadership [and with] the way they think."

The privacy professional suggested developing a joint risk matrix, involving internal auditors and the privacy and security teams, to help clarify complex language and align privacy and data security with the organization's broader risk management initiatives.

This collaborative matrix could help manage the dynamic risks associated with privacy and security and provide a visual representation that facilitates understanding for leadership. The goal would be to bridge the gap between technical discussions about laws, definitions, and other gray areas and make the information more accessible.

Bridging the gaps

Contextual differences between privacy professionals and senior leadership can arise as a result of their distinct perspectives and priorities. Following are some examples of these common differences.

	Privacy professionals	Senior leadership
Technical versus business language	Often use technical and legal terms when discussing privacy and data protection principles, practices, and compliance	Generally prefer more business-oriented language focused on risks, opportunities, and strategic decision-making
Detail-oriented versus high-level	Often delve into the details of privacy policies, data processing activities, and legal requirements	Might prefer high-level summaries and overviews that highlight the key implications and business impact of privacy initiatives
Legal versus practical	Generally emphasize legal requirements and the need for strict compliance	Can be more concerned with practical implementation, cost-effectiveness, and finding a balance between privacy and business needs

Source: Crowe analysis, February 2024

Aligning perspectives and objectives

A recurring theme throughout the discussion was the need to understand the slightly diverging perspectives of the internal audit and privacy functions. The two perspectives intersect but are not identical, often resulting in some differences in priorities. Internal audit focuses on more broad-based risks, while a privacy function owns a slice of that risk in the organization.

At their core, however, the two functions are working toward a common goal, as one of the information security participants observed.

"The entire goal is to improve the organization," he said. "We all do it slightly differently, but if we have the same goal, then it benefits the data subjects – because we're protecting their data – but it's also benefiting the organization because we're improving security, we're improving privacy, [and] we're improving compliance. And generally, we're just getting better every step of the way."

A shared objective is advantageous for both data subjects and the organization. It ensures the protection of data subjects' data and enhances the organization's security, privacy, and compliance. The ongoing process of continual improvement is viewed as integral to the organization's sustained development.

One of the internal audit professionals drew parallels between the approach taken by auditors in addressing fraud awareness and the necessity for a similar approach to data privacy awareness. Comparing it to the ubiquity of fraud considerations, he emphasized the need for data privacy awareness to permeate all areas and levels within the organization. Building on the importance of a shared objective, the need for comprehensive awareness extends beyond individual roles.

"It's like fraud [in that] it has to be there everywhere," he said. "Everything you do, there's an angle of privacy to it. It's that mindset, and we have to train ourselves to always look out for privacy … always keeping that at the back of our mind as we are looking at things … subconsciously thinking, 'Does this have a privacy impact?'"

"It should be a part of every audit program you have," he observed. "[For] every audit you execute, to some extent, you should listen for privacy implications in every conversation you have. Whether it's a walk-through or an issue discussion or a conversation with somebody that's trying to implement a new process and getting your input. … That's how I perceive the role of internal audit there."

Accommodating organizational change

Both functions face another shared challenge: Both must adapt to a continually changing business environment.

“There’s a … perspective that really matters in this conversation,” one of the participating privacy professionals said. “And that is [that] the business is constantly changing.”

In addition to the evolving regulatory environment, most organizations are also undergoing constant change as they adapt to new challenges or seek out new opportunities, she explained. As a result, the enterprise’s overall risk picture is never static – and neither are the data protection and privacy components of that picture.

She emphasized that “The business is constantly changing. … Internal audit and privacy can bring their perspectives in that environment of constant change, and there [are] just a lot better results for the organization when that risk is mutually understood and both parts of the organization are trying to improve individual performance and reducing risk while they do it.”

At their core, internal auditors and privacy professionals are change agents. Helping their organizations in navigating change through effective communication provides tremendous benefits.

> The business is constantly changing. … Internal audit and privacy can bring their perspectives in that environment of constant change, and [there are] just a lot better results for the organization when that risk is mutually understood and both parts of the organization are trying to improve individual performance and reducing risk while they do it.
>
> *– Data privacy leader*

> You have those in internal audit that do talk directly to leadership, directly to the board, and sometimes that is different than where the … privacy professionals go in terms of reporting structure. But there are times where you put that ad hoc team … together, which includes general counsel, internal audit, the CISO, and a variety of people, and you have a much broader impact to the organization because they each report differently to leadership or to the board.
>
> *– Data privacy leader*

> Everything you do, there's an angle of privacy to it. It's that mindset, and we have to train ourselves to always look out for privacy … always keeping that at the back of our mind as we are looking at things … subconsciously thinking, "Does this have a privacy impact?"
>
> *– Internal audit leader*

> Even though we're each doing our individual jobs, we're going to the same goal. But because we each report differently to the organization at times, then we can have a much broader support base for those initiatives.
>
> *– Data privacy leader*

Resources offered by The IIA

For relevant guidance, we encourage you to explore the valuable resources provided by The Institute of Internal Auditors.

Auditing Identity and Access Management

Auditing Cybersecurity Operations: Prevention and Detection

IT Essentials for Internal Auditors

Conclusion and recommendations

The overarching consensus that emerged from the roundtable discussion and formed the foundation for this report revolved around the importance of promoting effective collaboration between internal audit and privacy professionals. An equally critical conclusion was the need to develop a front-of-mind awareness of data protection and privacy risks across all parts and at all levels of the organization. While acknowledging the challenges inherent in integrating data privacy discussions into the audit process, participants emphasized the need to work together to make sure the organization is committed to data privacy.

The evolving landscape of privacy regulations, coupled with increasing recognition of an individual's ownership of their personally identifiable data, necessitates a shift in organizational perspectives. From the internal audit standpoint, the discussion emphasized the importance of making data privacy a higher priority.

As the discussion concluded, one of the internal audit leaders urged his colleagues to take a more proactive approach toward data privacy, describing how he intends to upgrade his own team's approach.

"During the audits, when we find something, we reach out to the data privacy office and ask, 'Is that a breach or not a breach?' and then we raise red flags," he explained. "But what we really should do is now really incorporate that into our audit universe, give it a higher priority, and work with the data privacy office to build a robust program."

That program should incorporate risk and control matrices that are specific to data privacy issues, he said.

"What are the risks, what are the possible controls there, and what are the compliance standards? That's how we build together the data privacy [effort] internally," he said.

Rather than treating data privacy as an ad hoc concern during audits, the proposal is to incorporate it systematically into every audit program. This effort requires collaborating with the data privacy office to establish a robust program that integrates risk and control matrices tailored to data privacy issues.

The ultimate objective, as articulated by the roundtable participants, is a collective effort to improve the organization. Alongside proactive outreach, internal audit professionals can pursue several specific initiatives, including actively listening for privacy implications in every aspect of their work. By doing so, internal auditors can contribute significantly to the organization's success in adapting to the ever-changing business environment and addressing the multifaceted aspects of data privacy. Ultimately, the shared commitment to a common goal – improving the organization – highlights the collaborative efforts required to achieve success in privacy, security, and compliance initiatives.

Internal Audit Foundation

About the Foundation

The Internal Audit Foundation provides insight to internal audit practitioners and their stakeholders, promoting and advancing the value of the internal audit profession globally. Through the Academic Fund, the Foundation supports the future of the profession through grants to support internal audit education at institutions of higher education. For more information, visit theiia.org/Foundation.

2023-24 Board of Trustees

President
Warren W. Stippich Jr., CIA, CRMA

Senior Vice President, Strategy
Glenn Ho, CIA, CRMA

Vice President, Finance and Development
Sarah Fedele, CIA, CRMA

Vice President, Content
Yulia Gurman, CIA

Trustees
Hossam El Shaffei, CCSA, CRMA
Reyes Fuentes Ortea, CIA, CCSA, CRMA
Nora Kelani, CIA, CRMA
Shirley Livhuwani Machaba, CCSA, CRMA
Raoul Ménès, CIA, CCSA, CRMA
Hiroshi Naka, CIA
Anthony J. Pugliese, CIA
Bhaskar Subramanian

Staff liaison
Laura LeBlanc, Senior Director, Internal Audit Foundation

2023-24 Committee of Research and Education Advisors

Chair
Yulia Gurman, CIA

Vice-Chair
Jane Traub, CIA, CCSA, CRMA

Members
Tonya Arnold-Tornquist, CIA, CRMA
Christopher Calvin, CIA
Jiin-Feng Chen, CIA
Andre Domingos
Christina Duquette, CRMA
Marc Eulerich, CIA
Dagmar Flores, CIA, CCSA, CRMA
Anargul Kairulla, CIA
Ayaka Mitsunari
Ahmed Mohammed, CIA
Grace Mubako, CIA
Ruth Doreen Mutebe, CIA
Thomas O'Reilly
Erika C. Ray, CIA
Brian Tremblay, CIA
Koji Watanabe

Staff liaisons
Nicole Narkiewicz, Senior Manager, Research and Insights, The IIA
Deborah Poulalion, Senior Manager, Research and Insights, The IIA

Published February 2024.

CDUW2499-002C

Crowe

Internal Audit FOUNDATION