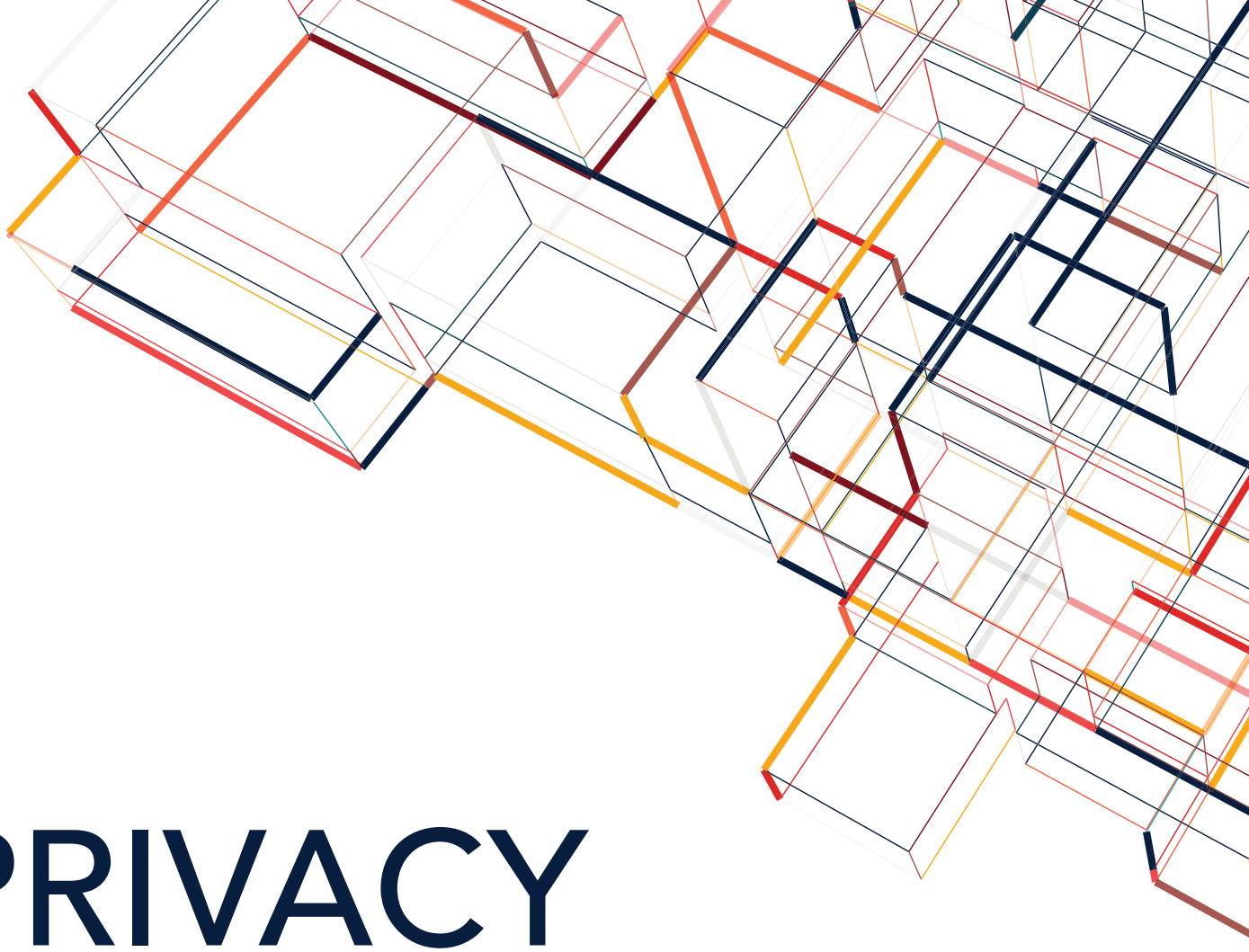


PRIVACY AND DATA PROTECTION

Part 2: Internal Auditors' Views on Risks, Responsibilities, and Opportunities

R. Michael Varney, CPA, CIA; Adam Pajakowski, CIPM, CFE, CIA; and Amanda M. Marderosian

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.

ISBN-13: 978-1-63454-135-0
26 25 24 23 22 1 2 3 4 5 6

Table of contents

Introduction and executive summary

As the second part of a three-part series of research activities, this report builds on a foundation laid in early 2020 with the publication of "Privacy and Data Protection Part 1: Internal Audit's Role in Establishing a Resilient Framework." Where the stated purpose of that report was to assist internal auditors in assessing their current level of preparedness regarding privacy and data protection issues, the purpose of this report is to present the findings of an Internal Audit Foundation (Foundation) survey and field interviews to examine how internal audit as a profession is responding to these issues.

As noted in Part 1 of this series, privacy and data protection have become critical areas of concern for all types of organizations – large and small, public and private, commercial and not-for-profit. The International Association of Privacy Professionals (IAPP) notes that privacy, which Supreme Court Justice Louis Brandeis famously defined as the "right to be let alone," actually encompasses several related concepts including information privacy, bodily privacy, territorial privacy, and communications privacy.[1] Of these four areas, information privacy is most directly affected by an organization's data protection policies and practices.

The IAPP's glossary also makes an important distinction between data protection and data security. Data protection – which the IAPP defines as "the rules and safeguards applying under various laws and regulations to personal data about individuals that organizations collect, store, use and disclose" – extends beyond just securing information to also include "devising and implementing policies for its fair use."[2]

In order to develop a better understanding of internal auditors' perceptions of these concepts, the Foundation authorized a survey among chief audit executives (CAEs) and audit directors, which was conducted Sept. 9-17, 2021. The first section of this report provides more in-depth information on the size and nature of the survey respondents' organizations.

As explained in the analysis in subsequent sections of this report, the responses to the survey suggest that a number of likely opportunities exist where internal auditors could add value to their enterprises – while also building, developing, or strengthening their critical relationships with peers elsewhere in their organizations – by taking a more active leadership role in mitigating data privacy risk.

More specifically, this report explores ways in which internal audit can become involved earlier in the data security and privacy processes, providing both guidance and support to the initial risk assessment and remediation activities. These functions need to be performed, of course, without jeopardizing the essential objectivity and independence that are hallmarks of the internal audit profession.

Another overarching observation about the survey responses relates to the rapidly evolving regulatory environment in which the survey was conducted. Along with the obvious effects that COVID-19 pandemic-driven changes to work environments and work processes have had on data privacy concerns, a number of new regulatory regimens have also arisen in the months since Part 1 of this series was published.

These developments include, for example, Brazil's new General Data Protection Law, which was passed in mid-2018 but went into effect in early 2020,[3] and China's Personal Information Protection Law, which went into effect Nov. 1, 2021.[4] Within the United States, new state-level data privacy regulations include the Virginia Consumer Data Protection Act, signed into law in March 2021,[5] the Colorado Privacy Act, enacted in July 2021, and others.[6]

Although these various jurisdictions' data privacy requirements have many similarities, their variations can present significant compliance challenges to organizations whose scope of operations or customer bases make them subject to several competing and slightly different regulatory regimens. Some of the survey responses and comments reflect those challenges, along with the maturation of more established privacy regulations such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018.

Now that organizations have had several years' experience in developing and implementing privacy frameworks to comply with these more mature standards, internal auditors may expect increasing demand for them to review their organizations' compliance efforts and provide assurance of both their adequacy and effectiveness. In that environment, this review of the current state of the profession as it relates to privacy and data protection concerns can provide a useful baseline for measuring and guiding internal audit's growing involvement in this critical area of risk.

---

[1] "Glossary of Privacy Terms," International Association of Privacy Professionals online resource, https://iapp.org/resources/glossary/

[2] Ibid.

[3] Renato Leite Monteiro, "The New Brazilian General Data Protection Law – A Detailed Analysis," International Association of Privacy Professionals Privacy Tracker, Aug. 15, 2018, https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/

[4] Josh Horwitz, "China Passes New Personal Data Privacy Law, to Take Effect Nov. 1," Reuters, Aug. 20, 2021, https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/

[5] Sarah Rippy, "Virginia Passes the Consumer Data Protection Act," International Association of Privacy Professionals Privacy Tracker, March 3, 2021, https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/

[6] Sarah Rippy, "Colorado Privacy Act Becomes Law," International Association of Privacy Professionals, The Privacy Advisor, July 8, 2021, https://iapp.org/news/a/colorado-privacy-act-becomes-law/

1) About the survey participants

The IIA's Internal Audit Foundation emailed survey invitations to CAEs and directors throughout North America and also publicized the survey through a social media campaign. Seventy-six people completed the survey: 78% were CAEs or equivalent, while the other 22% were either directors or senior managers who have responsibility for assurance services.

Participants also were asked for information regarding the size and scope of their organizations' internal audit functions and about the general size and nature of the organizations themselves. These questions revealed the following characteristics:

- The survey respondents' internal audit departments ranged in size from as few as one to five full-time equivalents (FTEs) to as many as 21 or more FTEs. Although many of the departments were on the lower end of that range, a sizable portion (29%) of them had 11 or more FTEs. This broad range suggests that the issues, concerns, and observations the participants noted would apply to a good cross-section of the profession.
- Roughly half of the responding audit executives' organizations employed large workforces (more than 1,500 FTEs). At the other end of the spectrum, one-third of the organizations had 500 or fewer employees. Again, this range suggests the survey findings would have broad applicability.
- The survey population encompassed a range of enterprise types. Public sector agencies, publicly traded businesses, and privately held businesses were represented in roughly equal portions, with not-for-profit organizations accounting for another significant segment of the population, as shown in Exhibit 1.

Exhibit 1: Survey respondents' organization

Public sector (including federal, state, and local government-sponsored enterprises)	30%
Publicly traded (listed) organizations	29%
Privately held (not listed) organizations	25%
Not-for-profit organizations	12%
Other	4%

Source: Internal Audit Foundation/The IIA/Crowe, Privacy and Data Protection survey, September 2021.

n = 76.

Within the survey population there was especially strong representation from the finance and insurance industries, which accounted for slightly more than one-third of the participants. Educational services (16%) and public administration (9%) also had relatively high representation compared to other industries.

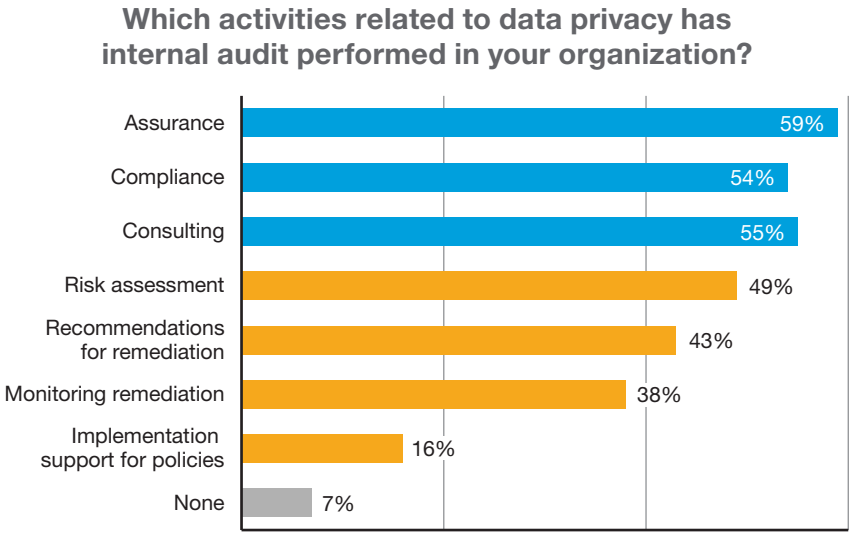
2) Data privacy roles and responsibilities

The survey responses reveal that the majority of internal auditors are engaged in at least some internal audit activities related to data privacy, but the responses also suggest some possible opportunities for greater involvement.

Internal audit data privacy activities

Overall, 93% of survey respondents said they have performed at least one type of internal audit activity related to data privacy (Exhibit 2). When asked to specify which activities they were engaged in, more than half said they had performed assurance, compliance, and consulting-type activities related to data privacy. But fewer than half have performed data privacy risk assessments or activities related to risk remediation such as making recommendations or monitoring remediation activities.

Exhibit 2: Internal audit activities



Source: Internal Audit Foundation/The IIA/Crowe, Privacy and Data Protection survey, September 2021.

n = 76.

One factor that likely contributed to internal auditors' greater engagement in assurance, compliance, and consulting activities (when compared to risk assessment and remediation) is the profession's traditional and legitimate concern over maintaining objectivity and independence. Looking forward, however, the survey responses also suggest that opportunities exist for the internal audit function to expand its activities as a value-adding partner in addressing data privacy risk, in addition to its mandated assurance and consulting activities.

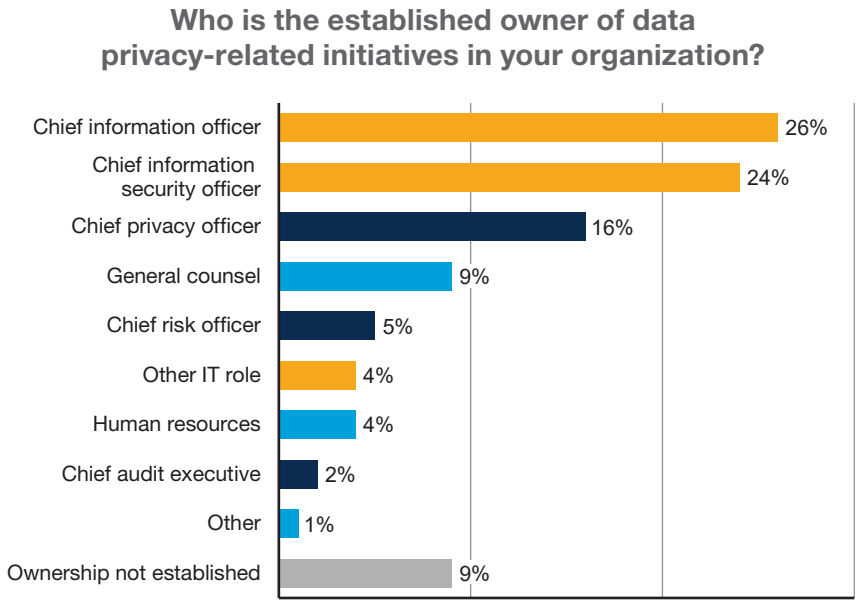
In particular, it appears internal auditors often might become more involved earlier in the overall data privacy risk management process. For example, internal audit can provide insights that could be particularly helpful in enabling process owners to identify and quantify risks so they can more effectively prioritize and allocate resources. Internal audit also can offer valuable feedback and guidance on data privacy policies and governance issues. Such early involvement could help internal auditors build or strengthen their internal relationships with other departments and business functions within their organizations.

Internal audit departments can take on these roles without sacrificing their essential objectivity. Section 6 of this report discusses this concept further and offers additional examples of how some organizations are pursuing these suggested opportunities.

Data privacy ownership

In addition to concerns over independence, it is likely that internal auditors' views of their involvement in data privacy activities also reflect their understanding of data privacy responsibilities within their organizations. As shown in Exhibit 3, more than half of the survey respondents (54%) say data privacy initiatives are owned by the information technology (IT) function, as represented by either the chief information officer, chief information security officer, or some other role within the IT organization.

Exhibit 3: Data privacy ownership



Source: Internal Audit Foundation/The IIA/Crowe, Privacy and Data Protection survey, September 2021.

n = 76.

Assigning ownership of data privacy risk management to the IT function exposes organizations to a number of potential weaknesses. IT priorities are understandably and properly oriented toward maintaining system effectiveness and operability, including the maintenance of data security and integrity. While the technology for protecting data privacy falls within this realm, the regulatory and compliance implications do not, and IT personnel are inherently less focused on regulatory concerns.

In one sense, IT's continued widespread ownership of data privacy responsibilities also could be considered somewhat surprising. The continually growing number of new data privacy regulatory regimens would seem to suggest that organizations would be wise to begin viewing data privacy more from a regulatory and compliance standpoint rather than as primarily a data concern. For example, some regulations require an assigned data protection officer (DPO) or one main privacy contact.

Helping to refocus senior management's understanding of this shift is another way that internal auditors can add value to their organizations. Even if an organization is not subject to the GDPR, which if applicable could require the appointment of a DPO, it could nevertheless benefit from assigning data privacy responsibilities to a compliance-oriented executive, such as a chief risk officer or chief privacy officer (as reflected in only 5% and 16% of the survey responses).

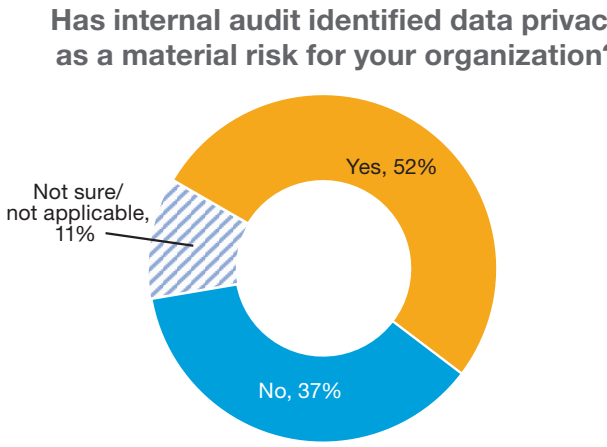
Finally, 9% of the respondents said their organizations had not established ownership of data privacy initiatives. Such situations present an obvious opportunity for internal audit to step up and urge management to take a more proactive approach to this area of risk management.

3) Data privacy as a material risk

Survey respondents' opinions regarding the materiality of data privacy risk – and their stated reasons for those opinions – raise several questions that are worth exploring. To begin the discussion, just over half of the survey respondents (52%) reported that their internal audit functions had identified data privacy as a material risk for their organizations. See Exhibit 4.

"Material risk" was defined in the survey as a "capital-related downside risk that, based on the institution's internal definitions, has a material impact on its overall risk profile and may affect the capital adequacy of the institution."[1]

Exhibit 4: Materiality of data privacy risk



Source: Internal Audit Foundation/The IIA/Crowe, Privacy and Data Protection survey, September 2021.

n = 76.

This number is somewhat surprising, especially when viewed alongside other recent research in this area. For instance, in the 2022 edition of The Institute of Internal Auditors' annual OnRisk report, board members, CAEs, and other C-suite executives were asked to rate the relevance of various risks on a scale of 1 to 7. When asked to rate data privacy risk, 77% of the participating CAEs and board members rated it either 6 or 7, the highest relevance ratings.[2]

The OnRisk rating appears to present a significant disparity with this survey's findings, but digging deeper into the OnRisk responses provides some potential explanation for the difference. For example, only 33% of CAEs gave a high rating to their organizations' capabilities in this area, and only 53% gave themselves a high rating regarding their personal knowledge of data privacy issues.

Viewing both surveys' responses in this context, it could be argued that internal auditors' views regarding the responsibility for data privacy within their organizations (as discussed in Section 2), coupled with uncertainty about their own understanding of data privacy issues (as revealed by the OnRisk responses), might be leading them to underestimate the level of risk associated with data protection and privacy issues.

Of particular interest are some of the specific concerns raised by CAEs and directors who identified data privacy as a material risk. Their open text responses were analyzed and grouped into general categories. The five most commonly cited concern areas were:

1. Regulatory requirements
2. Risk to reputation
3. The sensitivity or importance of the data held by their organizations (such as personal financial or healthcare information)
4. Decentralization of data systems and a lack of consistent procedures
5. The generally increasing likelihood of data breaches

Some of the participants' most revealing text comments are shown here:

> "From an inherent risk standpoint, privacy is an absolute necessity for our organization, both because of the reputational and financial impact a significant privacy event could have on our company as well as the regulatory impact (including fines and penalties) should regulators determine we have inadequate privacy practices in place. Because we are a financial services institution, we are stewards of a multitude of sensitive information that our clients expect to be treated with the utmost care and confidentiality. A privacy breach could have a significant impact on our clients' trust in the firm and would take significant effort and money to repair."
>
> *– Publicly traded financial services institution*

> "In our increasingly virtualized operating environment (including remote work, cloud computing, and SaaS/IaaS), the potentially significant impacts and inherent risk resulting from data breaches or noncompliance with numerous, growing, and overlapping data privacy regulations are coupled with ongoing maturation of the regulatory bodies and jurisprudence, and a higher likelihood due to the increased prevalence of and reliance on technology. These all lead to a higher risk profile for our organization."
>
> *– Large not-for-profit organization*

> "We handle a high volume of data using a decentralized approach to management with multiple legacy and source systems of data owned by multiple business units."
>
> *– Medium-sized publicly traded company*

> "Our policies and practices are improving rapidly but are still not fully in place and lack a data governance framework. In addition, third-party risk involving suppliers and partners is a significant concern in protecting our data."
>
> *– Medium-sized privately held business*

> "We have a very decentralized structure from an operational and IT perspective, with thousands of data owners and hundreds of systems. As a large research institution with an academic medical center, all types of data including personally identifiable information, protected health information, and payment card industry requirements are in play."
>
> *– Large public sector organization*

4) Internal auditors' views of program effectiveness

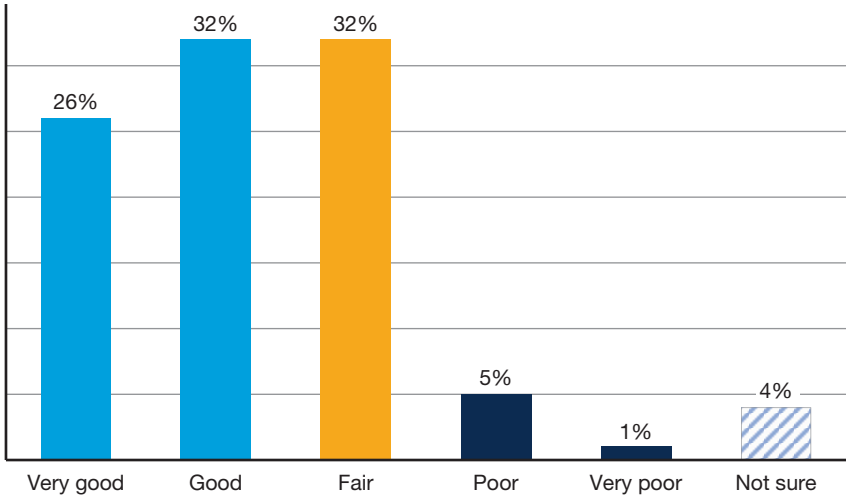
Survey participants were asked several questions regarding their perceptions of the effectiveness of their organizations' data privacy and protection efforts. Their responses raise several questions that should be of concern to the profession, and they merit further discussion.

Quality of data privacy policies

When audit executives were asked for their opinions about the quality of their organizations' data privacy policies, barely half (58%) of the survey respondents rated their policies as good or very good, as shown in Exhibit 5. In view of earlier responses indicating that data privacy is widely regarded as an IT-owned function, this response could reflect a perception that data privacy policy issues are largely technical in nature, rather than regulatory concerns.

Exhibit 5: Quality of data privacy policies

How would you describe the quality of your organization's data privacy policies?



Source: Internal Audit Foundation/The IIA/Crowe, Privacy and Data Protection survey, September 2021.

n = 76.

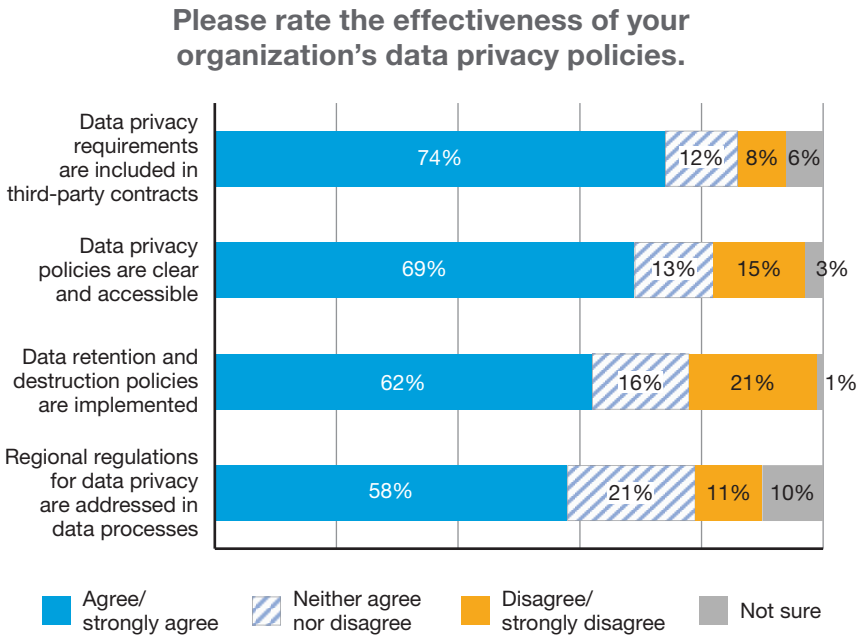
Put another way, almost four out of 10 (38%) said their policies were just fair or worse, and 4% were unsure what to think. In part, this finding relates back to the survey participants' response to the earlier question about ownership of data privacy initiatives. As noted in Section 2, a majority of respondents said their organizations assigned ownership of these issues to the IT department, rather than to risk management functions. This situation again suggests that internal auditors can provide value to their organizations by engaging earlier in the data privacy process, and becoming more proactively involved in policy updates, in addition to assessing the quality of data privacy policies as part of their compliance function. Section 6 of this report expands on this potential role for internal audit.

Policies versus practices

When survey respondents were asked about the specifics of their data privacy programs, opinions differed about the effectiveness of their policies (Exhibit 6) and the effectiveness of their practices (Exhibit 7). In general, auditors gave higher marks to their organizations' policies than their practices, which suggests that policies might be in place but are not enforced or executed effectively.

For example, 69% of the survey respondents either agreed or strongly agreed that their organizations' privacy policies are clear and accessible, and 74% of respondents either agreed or strongly agreed that data privacy requirements are included in third-party contracts.

Exhibit 6: Effectiveness of data privacy policies

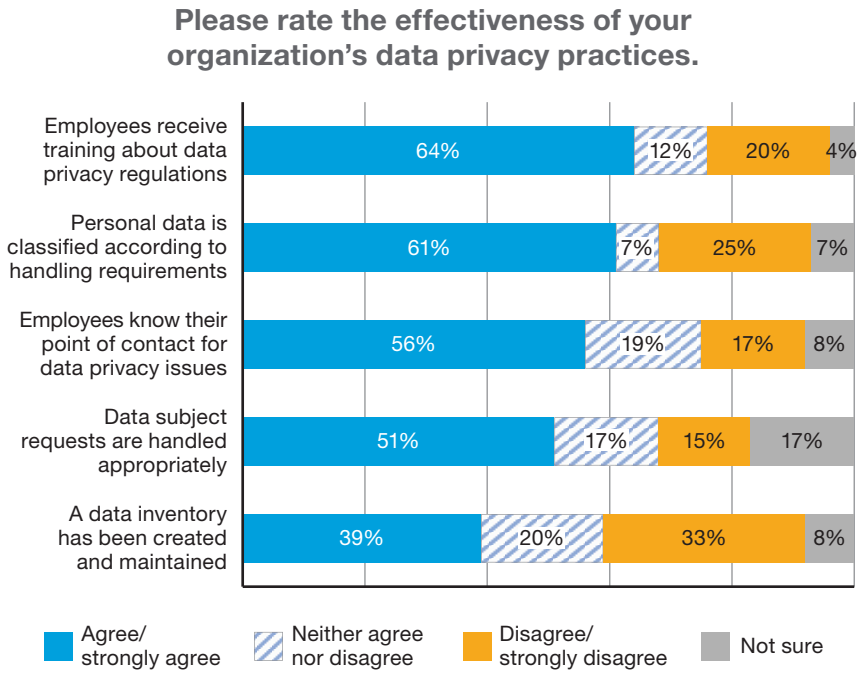


Source: Internal Audit Foundation/The IIA/Crowe, Privacy and Data Protection survey, September 2021.

"Not applicable" responses were excluded. *n* = 71 to 76.

But when asked about specific data privacy practices, some weaknesses were exposed, particularly in the areas of data inventory and classification practices. For example, only 39% of respondents agreed or strongly agreed that data inventories are created and maintained, even though an accurate and complete data inventory is a critical and typically the first component of any data privacy framework. This could mean the policies for areas such as data inventories do not exist or are not formally executed and adhered to.

Exhibit 7: Effectiveness of data privacy practices



Source: Internal Audit Foundation/The IIA/Crowe, Privacy and Data Protection survey, September 2021.

"Not applicable" responses were excluded. *n* = 72 to 75.

Responses to survey questions about other basic issues also raised concerns. For example, when asked if personal data is classified according to handling requirements, one out of four (25%) disagreed. This percentage would appear to be a very high failure rate for something that is an essential early step in any data privacy initiative. And barely half (51%) of the respondents agreed that data subject requests are handled appropriately in their organizations – again, a notably low level of effectiveness for such a basic requirement.

While 64% of respondents said their organizations' employees receive training about privacy and data protection regulations, it is somewhat concerning that only 56% said their companies' employees know their point of contact for data privacy issues. This response raises doubts about the adequacy of these privacy training programs, since knowing who to contact if they have concerns would seem to be a very basic component of any employee training effort.

Taken together, these various responses suggest a number of opportunities for internal audit professionals to take a more active role in helping their organizations develop more effective privacy policy programs and practices, in addition to their assurance activities.

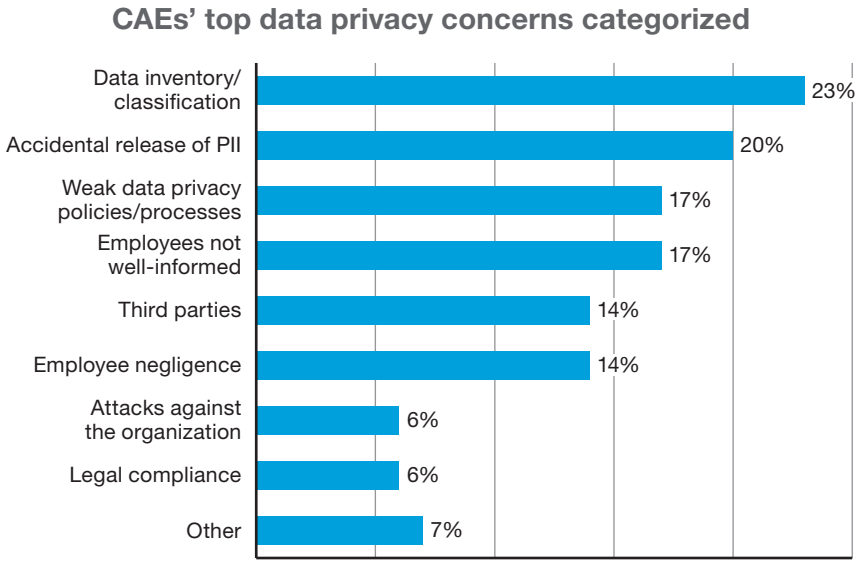
5) Internal auditors' most critical concerns

In view of the survey participants' responses to earlier questions, the logical next follow-up question in the survey was an open-ended question regarding what they view as top concerns related to data privacy at their organizations. As with the earlier open-ended question described in Section 3, the respondents' text responses to this question also were analyzed and categorized into commonly recurring themes.

Top concerns varied widely, but data inventory and classification was cited by the largest number of those responding (23%). This is not altogether surprising, given the earlier observation that only a minority of respondents said their organizations maintain data inventories. As mentioned in Section 4, creating data inventories and classification are key first steps in establishing a formal privacy program. When these activities are not done, items such as data deletion and data breach processes become more difficult.

As shown in Exhibit 8, other leading concerns included accidental release of personally identifiable information (20% of respondents), weak policies and processes in general (17%), and employees who were either not informed or poorly informed about data privacy issues (17%).

Exhibit 8: CAEs' top data privacy concerns



Source: Internal Audit Foundation/The IIA/Crowe, Privacy and Data Protection survey, September 2021.

The free response answers for this question were coded into categories. *n* = 35.

These are issues that all internal audit functions should consider as they review data privacy at their organizations. A review of individual responses reveals some potentially significant patterns. For example, in many cases, respondents who listed weak data privacy policies and processes as a top concern also expressed concerns about employees not being well-informed about privacy and data protection issues in general.

Moreover, even those respondents who believed sound policies were in place still expressed concerns about employees failing to follow guidelines or accidentally causing a breach. Representative comments illustrating internal auditors' concerns include the following:

> "Our highly decentralized environment means that a particular unit or department might or might not have done a data inventory and might or might not be aware of the policy or their responsibility to safeguard the data."
> – *Large public sector organization*

> "A top concern is the risk posed by individuals who inadvertently expose private data, either through an operational error or by falling victim to social engineering or other bad actor methods that allow private data to be compromised."
> – *Large publicly traded company*

> "There is a lack of effective classification and rules for different categories of classification and a lack of appropriate companywide training on data privacy."
> – *Medium-sized publicly traded company*

> "Incomplete data inventory prohibits an accurate risk assessment. There is a potential for data to reside on platforms that are not monitored."
> – *Other organization with fewer than 500 FTEs*

> "New employees might not be adequately prepared prior to having access to personal data of customers."
> – *Small privately held company with fewer than 500 FTEs*

6) How internal auditors can add value

In addition to addressing specific concerns and shortcomings they recognize in their organizations' data privacy programs, internal auditors also can take broader, more proactive steps to improve the overall effectiveness of privacy policies and practices. Although such efforts are distinct from their independent assurance responsibilities as risk management's third line, they nevertheless can be undertaken without impairing internal audit's ability to provide objective, unbiased assessments of risk and compliance.

In general, such efforts involve working with the owners of a data privacy program within their organization to assess and build out specific initiatives. Drawing on their own understanding of privacy regulations and requirements, most internal auditors are well positioned to help assess where the greatest data privacy risk lies – and thus where the data privacy owners or team can allocate resources most effectively.

Internal audit also can help the process owner identify which factors have the greatest impact on data privacy risk. In some organizations, a focus on certain physical locations might be most effective; in others, specific product or service lines require special attention; in still others, policy, personnel, or training issues merit review and enhancement. By helping the process owner identify these priorities, internal audit can help contribute to a more effective allocation of resources, while at the same time improving the overall effectiveness of the data privacy effort.

Beyond these general observations, industry experience offers several specific examples of how internal audit teams have applied these broad principles:

- **Risk assessment surveys.** One effective tool for helping to identify data privacy risks is an internal survey of key managers and executives. By asking targeted questions, the data privacy team and process owners can gain the insight needed to quantify the relevant risk and recognize potential mitigating solutions. In addition to contributing their extensive knowledge and understanding of the risks, internal auditors also can provide the initial impetus to launch such an effort, as well as help diagnose results for further compliance or audit efforts.
- **Policy review team.** In addition to reviewing privacy policies after they have been finalized as part of their audit function, many organizations have turned to internal audit for input during the policy development process. While the actual drafting of privacy policy is outside the scope of an objective internal audit function, audit executives can offer feedback and guidance as policies are being shaped. In addition, they can help gather other key privacy documents such as consent forms to ensure those items are refreshed and in line with policy updates.

- **Governance committee.** In many organizations internal audit plays a valuable role as part of a high-level data privacy governance committee. In addition to overseeing the basic structure and framework of the privacy program, such governance committees meet on a regular basis – typically quarterly – to address privacy risk concerns and any associated governance issues that arise. This is an opportunity for internal auditors to have a regular audience with board-level individuals and help advance the program through their insights.
- **Cross-training.** Just as internal audit departments often engage in temporary rotation of their personnel into the compliance office or other areas in the organization, a six-month rotation into the department that is responsible for data privacy compliance can provide both valuable experience and enhanced credibility. Auditors also can contribute significantly to developing and maturing the data privacy and protection program. Although such cross-training rotations are more workable in larger internal audit departments that have adequate resources to devote to such efforts, they also can be done less formally in smaller organizations.
- **Continuous monitoring and quality assurance.** One fundamental way internal audit can add value to an organization is through ongoing monitoring and review of compliance efforts, rather than limiting auditors' involvement to after-the-fact review and assessment. For example, GDPR Article 30 requires organizations to maintain records of processing activities if personal data is being collected, stored, or processed. Internal audit often can serve as a quality assurance partner, operating in real time to review how these processes are being documented and identify any gaps. As noted throughout the article, the formal data inventory and processing records needed to satisfy Article 30 appear to be an issue for organizations, so internal audit assisting in this area could have tremendous value.

  One common component of this effort is the distribution of privacy assessments to business process owners. Such assessments offer a structure or format that process owners can use to submit a high-level summary of the personal information being collected, any applications they use, and other relevant information as it relates to the associated personal data. By being part of the initial review process, internal audit can help see to it that the right questions are being asked, in addition to serving as a final check to validate all questions were answered.

Objectivity and lack of bias make internal audit an ideal partner in such efforts. Because internal audit has no direct or vested interest in the underlying business processes, it is able to provide detached guidance and counsel to process owners. Internal audit's objectivity can be particularly helpful in the governance and policy review functions mentioned earlier.

Conclusions and additional research

The joint IIA/Foundation/Crowe survey provided a number of insights that internal audit professionals can use to reflect on their own organizations' preparedness and effectiveness in managing risks associated with data privacy and protection.

Even more important, as this report described, an analysis of the survey responses reveals a number of potentially valuable opportunities for internal audit to take an earlier and proactive role in helping to recognize, manage, and mitigate these risks, while still fulfilling their role as defined by the International Professional Practices Framework:

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.[3]

By building on the initial research that was reported in Part 1 of this series and taking into consideration the opportunities described in this report, internal auditors can more effectively meet the challenges of adding value and improving their organizations' operations.

Looking forward, Part 3 of this series will examine how various stakeholders view data privacy issues and how they perceive internal audit's role and performance in this important area of risk. Through field interviews with privacy officers and other participants, the authors hope to uncover additional opportunities for internal auditors to contribute to their organizations' risk management, control, and governance processes.

---

[1] Law Insider online dictionary, https://www.lawinsider.com/search?q=material+risk

[2] "OnRisk: A Guide to Understanding, Aligning, and Optimizing Risk, 2022," Institute of Internal Auditors, 2021, https://na.theiia.org/periodicals/OnRisk/Pages/default.aspx?gclid=CjwKCAiAs92MBhAXEiwAXTi252EdF-IZEaJsoCRGKdE-XX6uZGLnyRSy_2l-rhdkTdTuC7cysZv78xoCFAcQAvD_BwE

[3] Institute of Internal Auditors Standards & Guidance, Code of Ethics, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx

Published February 2022.

The Internal Audit Foundation strives to be an essential global resource for advancing the internal audit profession. The Foundation's research and educational products provide insight on emerging topics to internal audit practitioners and their stakeholders and promote and advance the value of the internal audit profession globally. Through the Academic Fund, the Foundation supports the future of the profession by providing grants to students and educators who participate in The IIA's Internal Auditing Education Partnership Program. For more information, visit www.theiia.org/Foundation.

CFS2202-001A

Crowe

Internal Audit FOUNDATION