ISACA

Privacy in Practice 2024

Privacy

CONTENTS

ABSTRACT

Privacy in Practice 2024 reports the results of the ISACA global *State of Privacy Survey* conducted in the fourth quarter of 2023. This report focuses on privacy staffing, privacy operations, compliance, awareness training, privacy by design and breaches. While some survey findings are consistent with last year's survey results, others indicate that privacy teams may need to manage with fewer resources in the next year.

Executive Summary

Privacy in Practice 2024 explores privacy staffing, operations, compliance efforts, awareness training, breaches and privacy by design based on the results of the fourth annual ISACA global *State of Privacy Survey* conducted in the fourth quarter of 2023.

Respecting data subjects and protecting their privacy is a key component of digital trust. Additionally, failure to comply with privacy laws and regulations could result in significant fines and reputational harm. Privacy professionals who optimize their resources and build privacy into their products and services can gain a competitive advantage and protect their consumers. This survey report examines the state of organizational privacy.

Key Findings

This year's survey results reveal important insights for enterprises:

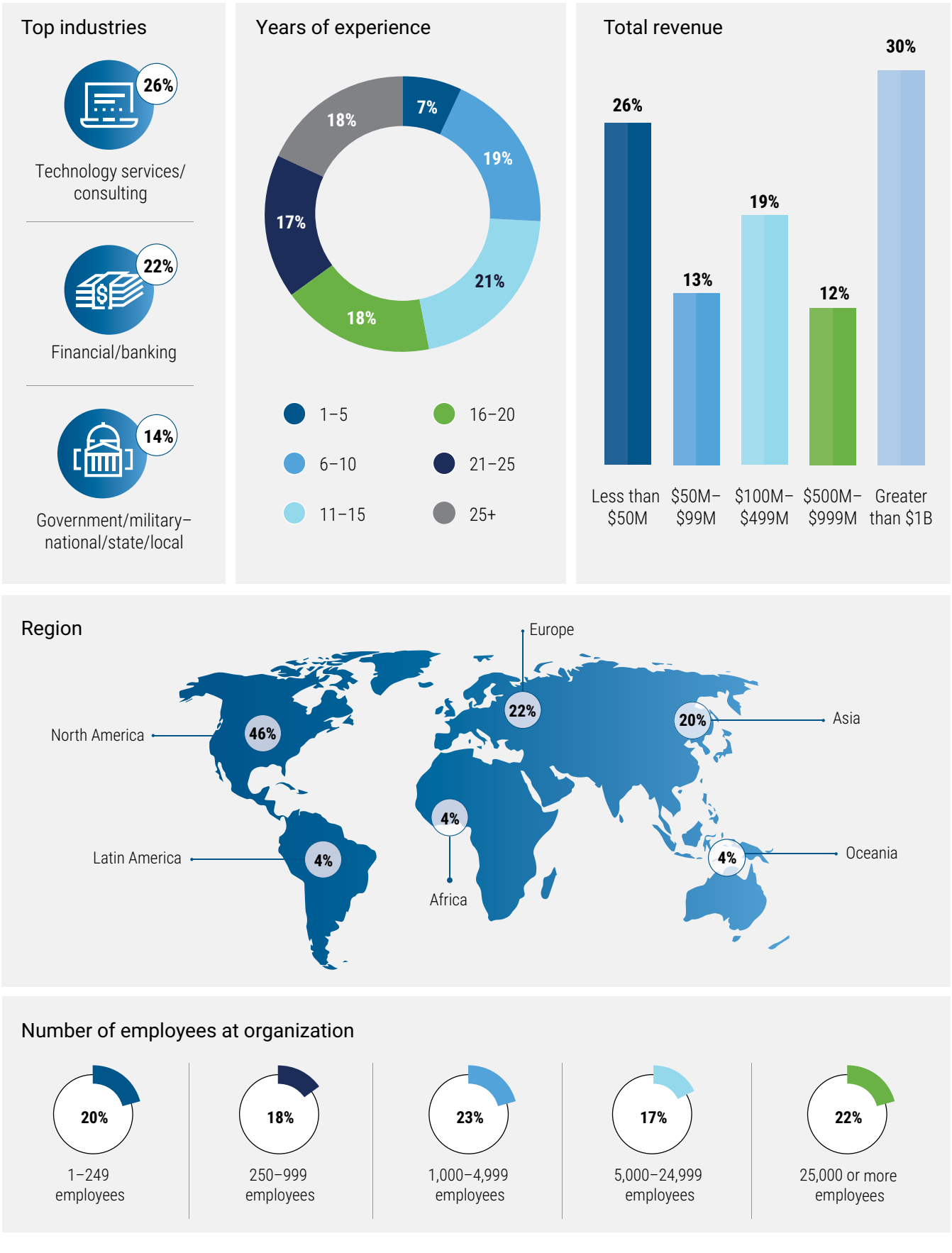
- Demand for technical privacy roles is significantly more likely to increase in the next year than demand for legal/compliance roles.
- Perceptions of funding and board prioritization of privacy are comparable to those reflected in last year's survey results.
- Expert-level privacy professionals are the most difficult to hire, consistent with last year's findings.
- The most common obstacles to creating privacy programs are a lack of competent resources; a lack of clarity on the program's mandate, roles and responsibilities; a lack of executive or business support; and a lack of visibility and influence within the enterprise.
- The most common privacy failure is poor or nonexistent training.
- This year's respondents were significantly more likely than last year's to believe their privacy budget would decrease in the next 12 months.
- Respondents identified the chief privacy officer role as the most likely to be accountable for privacy operations.
- Over one-third of respondents had no plans to use artificial intelligence (AI) to perform privacy-related tasks despite understaffing and lack of funding.
- Based on the survey responses, enterprises that practice privacy by design are more likely to:
  - Have more interaction across all functional areas of the organization
  - Have an organizational privacy strategy that aligns with other organizational objectives
  - Be confident in their organization's ability to ensure the privacy of its sensitive data
  - Feel their privacy budget is appropriately funded
  - Separate privacy training from security training

Privacy professionals who optimize their resources and build privacy into their products and services can gain a competitive advantage and protect their consumers.

Survey Methodology

In the fourth quarter of 2023, ISACA sent survey invitations to approximately 15,500 ISACA constituents who held the Certified Data Privacy Solutions Engineer™ (CDPSE™) designation or had "privacy" in their job title. Invitations were also sent to those who held the ISACA CSX Cybersecurity Practitioner Certification™ (CSX-P™) or Certified Information Security Manager® (CISM®) designation. More than 1,300 people completed the survey.

FIGURE 1: Respondent Demographics



Some respondents held multiple additional ISACA certifications. Thirty-nine percent of respondents were in management roles, 28 percent were in senior leadership roles, 20 percent were individual contributors, and the remaining 13 percent were in executive leadership positions. **Figure 1** shows additional demographic information about survey respondents.

Staffing Trends

Privacy professionals largely fall into two groups: legal/compliance professionals and technical privacy professionals. Legal/compliance professionals have expertise in the law and the ability to understand regulatory obligations. Technical privacy professionals have the skills and experience to evaluate and apply technical controls that can help achieve privacy objectives. In some enterprises, professionals in these roles work side-by-side on the same team, while in other enterprises, these roles are distinct functions that report to different executive leaders.

Technical privacy roles appear to be more understaffed than legal/compliance roles. Fifty-four percent of survey respondents said technical privacy roles were somewhat or significantly understaffed, while 44 percent of survey respondents said legal/compliance roles were somewhat or significantly understaffed. This is consistent with previous years' findings, in which technical privacy roles were typically more understaffed than legal and compliance roles. In this year's survey, the median privacy staff size was nine employees, compared to 10 last year, so it is not surprising that this understaffing trend is unchanged from last year's findings.

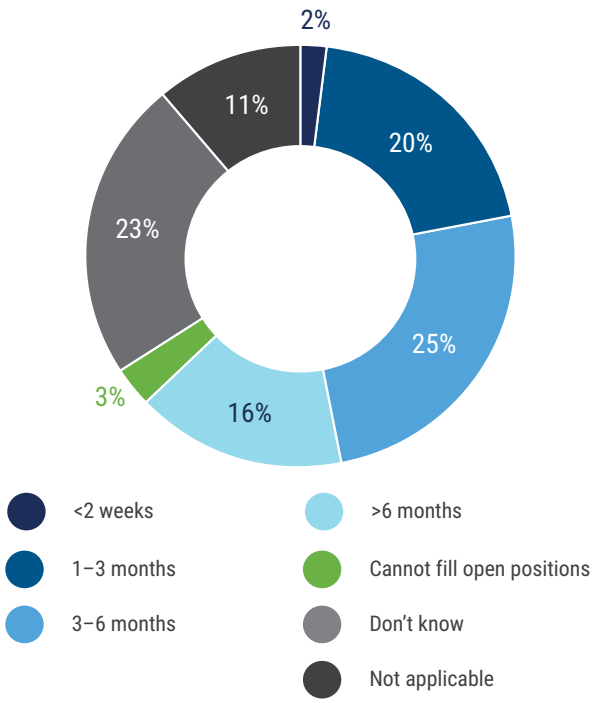
Open Privacy Positions

Many respondents indicated that their enterprises had open privacy roles. Twenty-five percent said their organizations had open legal/compliance privacy roles, and 31 percent reported open technical privacy positions. This is a slight decline from last year when 27 percent of respondents' organizations had open legal/compliance positions and 34 percent had open technical privacy positions. This is consistent with anticipated budget cuts; if privacy budgets are expected to decrease, it makes sense that hiring will slow down.

Figures 2 and **3** show the time required to fill privacy roles with a qualified candidate for legal/compliance and technical privacy roles, respectively. These findings are comparable to last year's.

FIGURE 2: Time to Fill Open Legal/Compliance Privacy Positions

On average, how long does it take to fill legal/compliance privacy positions with a qualified candidate?

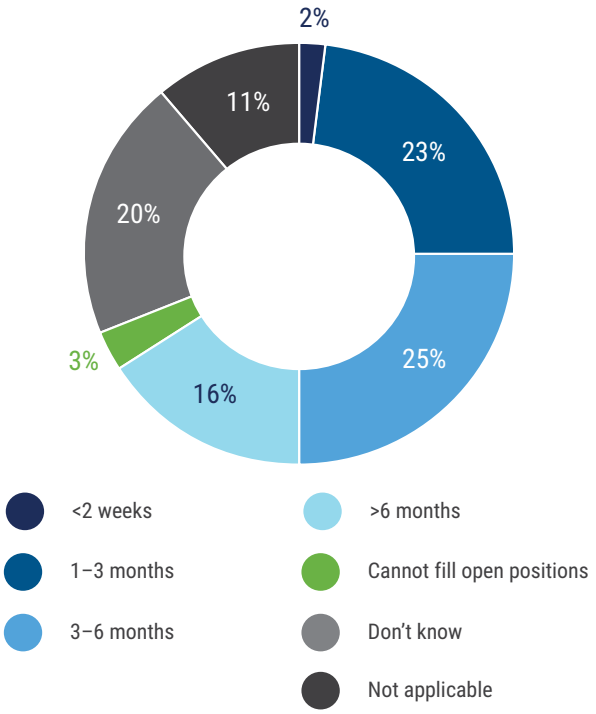


Eighteen percent of respondents said the time required to fill legal/compliance roles had somewhat or significantly

increased, which is identical to last year's findings. Nineteen percent of respondents said the time required to fill open technical privacy positions had increased. This represents a decline from last year when 23 percent of respondents said the time to fill open technical positions had somewhat or significantly increased.

FIGURE 3: Time to Fill Open Technical Privacy Positions

On average, how long does it take to fill technical privacy positions with a qualified candidate?



Qualifications

A major impediment to filling open positions is that many applicants are not considered well qualified. Only 21 percent of respondents indicated that more than half the applicants to legal/compliance roles and technical privacy roles in their enterprises were well qualified for position for which they are applying, compared to 24 percent for legal/compliance applicants and 25 percent for technical privacy applicants last year.

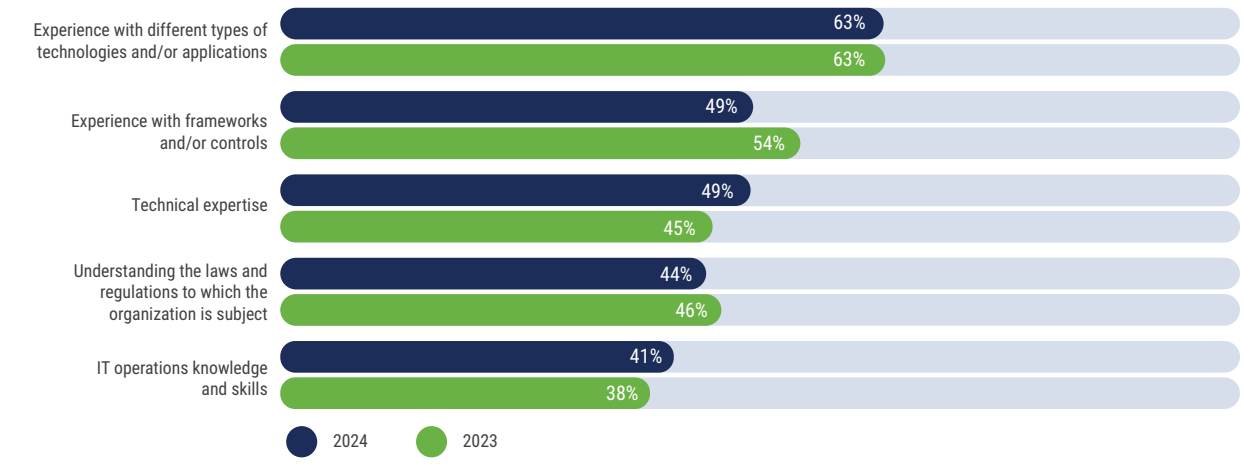
Figure 4 shows the top five skill deficiencies among privacy professionals as identified by survey respondents.

The top two deficiencies identified this year were the same as last year. However, the third-largest skill deficiency identified this year was technical expertise. Forty-nine percent of respondents identified technical expertise as a big skill gap, representing a 4 percent increase over last year. The fourth area of concern this year was understanding the laws and regulations applicable to an organization. Forty-four percent of respondents named it as a significant concern—2 percent lower than last year, when understanding laws and regulations was the third-biggest skill deficiency identified.

These results may signal a shift in hiring managers' expectations for privacy professionals. Possibly they understand that very few candidates with technical expertise will also have legal expertise, and they may

FIGURE 4: Identified Skill Deficiencies

In what areas do you see the biggest skill gaps in today's privacy professionals?



no longer be striving to hire a single person who can do everything. It is also possible that the rapidly evolving technology landscape has made technical expertise a more valuable candidate trait.

Figure 5 shows the importance of a variety of factors in determining a job applicant's qualifications and compares this year's findings to last year's. The figure shows the percentage of respondents who considered the factor in question to be very or somewhat important. Though survey respondents indicated that previous privacy experience was desirable in a candidate, the reality is that many practitioners pivoted to their careers in privacy. Forty-four percent of respondents said that more than half of their enterprise's privacy staff started their careers in a completely different field and transitioned to privacy roles. In fact, only 18 percent of respondents indicated that more than half of their enterprise's privacy staff began their careers in privacy.

These findings are consistent with the findings shown in **figure 6**, which illustrate the strategies enterprises use to address the privacy skills gap.

FIGURE 5: Importance of Factors in Determining an Applicant's Qualifications

How important are each of the following factors in determining if a privacy candidate is qualified?

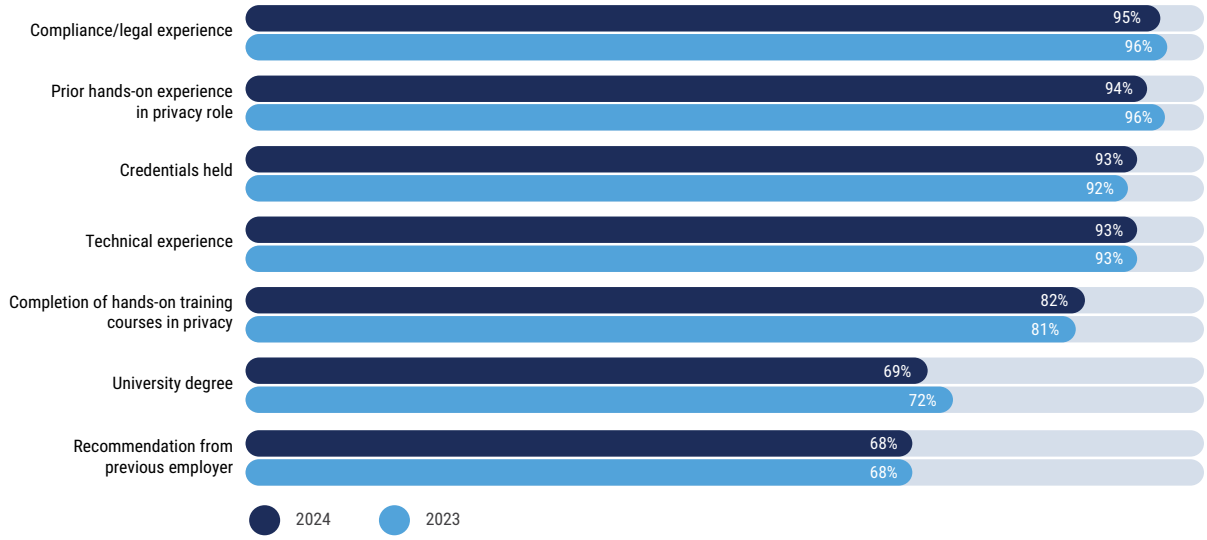
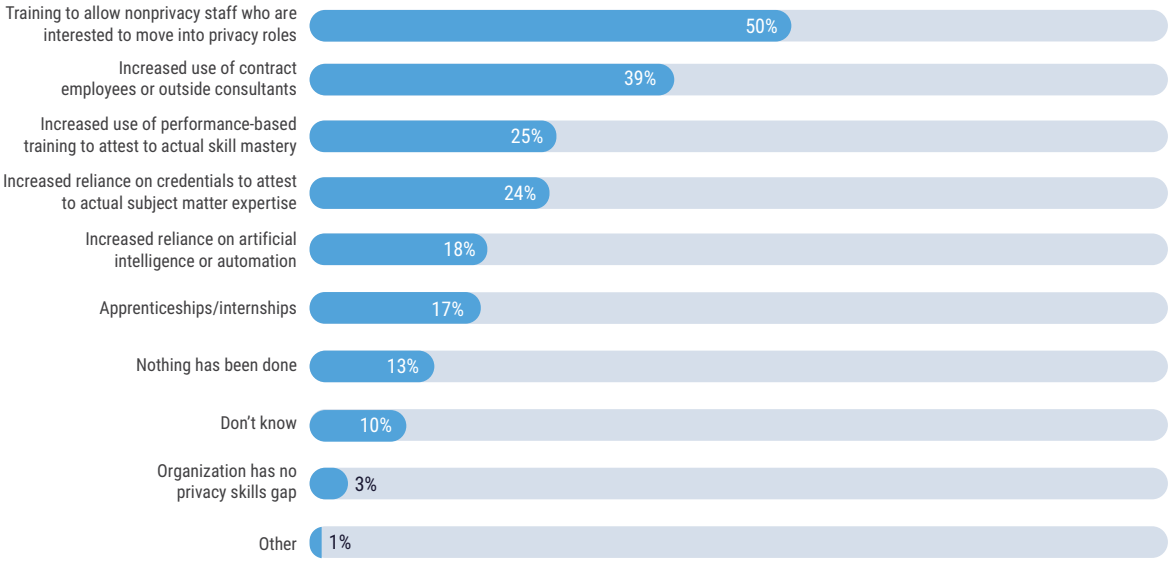


FIGURE 6: Actions Taken to Address Privacy Skills Gap

Which, if any, of the following has your organization undertaken to help decrease this privacy skills gap?



Demand for Privacy Professionals

Expert privacy professionals are the most challenging category to hire as evidenced by 76 percent of respondents, followed by practitioners (48 percent) and entry level/foundational privacy professionals (14 percent).

The demand for privacy professionals across all expertise levels is expected to increase over the next year. **Figures 7** and **8** show the anticipated demand for legal/compliance and technical privacy professionals over the next year, respectively. This year's respondents did not believe the demand would increase as significantly as last year's respondents did. Last year, 62 percent of respondents said they anticipated the demand for legal/compliance roles would increase, and 69 percent of respondents said the demand for technical privacy professionals would increase in the next year.

The increasing demand coupled with staff retention challenges could exacerbate understaffing issues in the future. Forty-one percent of respondents said they experienced difficulty in retaining qualified privacy professionals.

FIGURE 7: Demand for Legal/Compliance Privacy Roles

In the next year, do you see the demand for legal/compliance privacy roles increasing, decreasing or remaining the same?

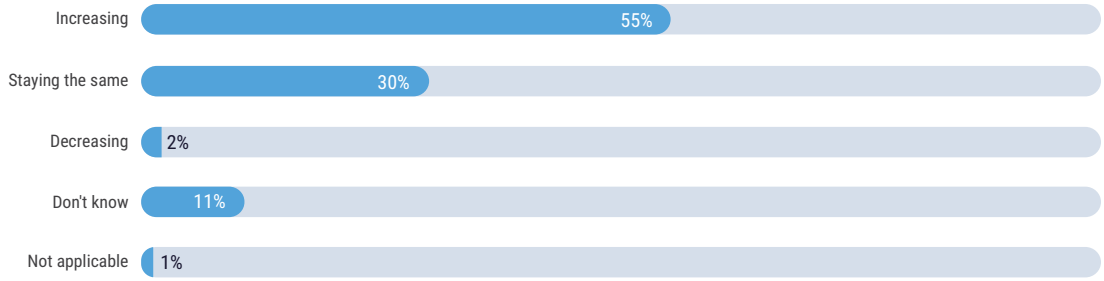
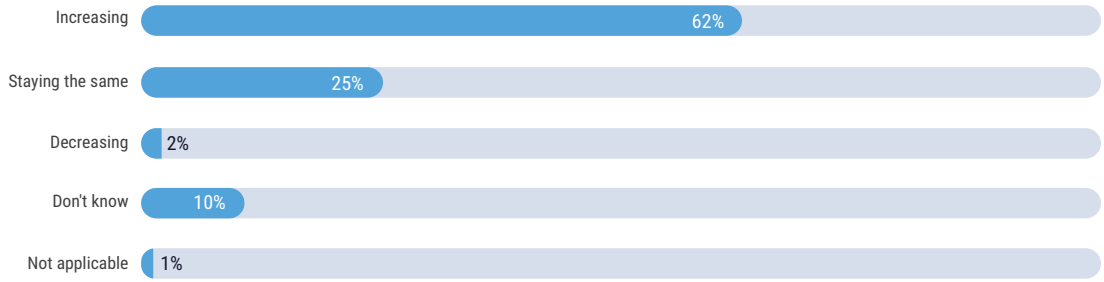


FIGURE 8: Demand for Technical Privacy Roles

In the next year, do you see the demand for technical privacy roles increasing, decreasing or remaining the same?



The demand for privacy professionals across all expertise levels is expected to increase over the next year.

Privacy Operations

To be successful, privacy programs require buy-in from the entire enterprise. Privacy professionals need to collaborate with nearly every department in their organization. The tone set at the top influences the enterprise's attitude and culture toward privacy. Enterprises with boards of directors that do not adequately prioritize privacy and that fail to provide it with the resources and funding it needs will likely experience challenges in accomplishing privacy objectives and meeting compliance requirements.

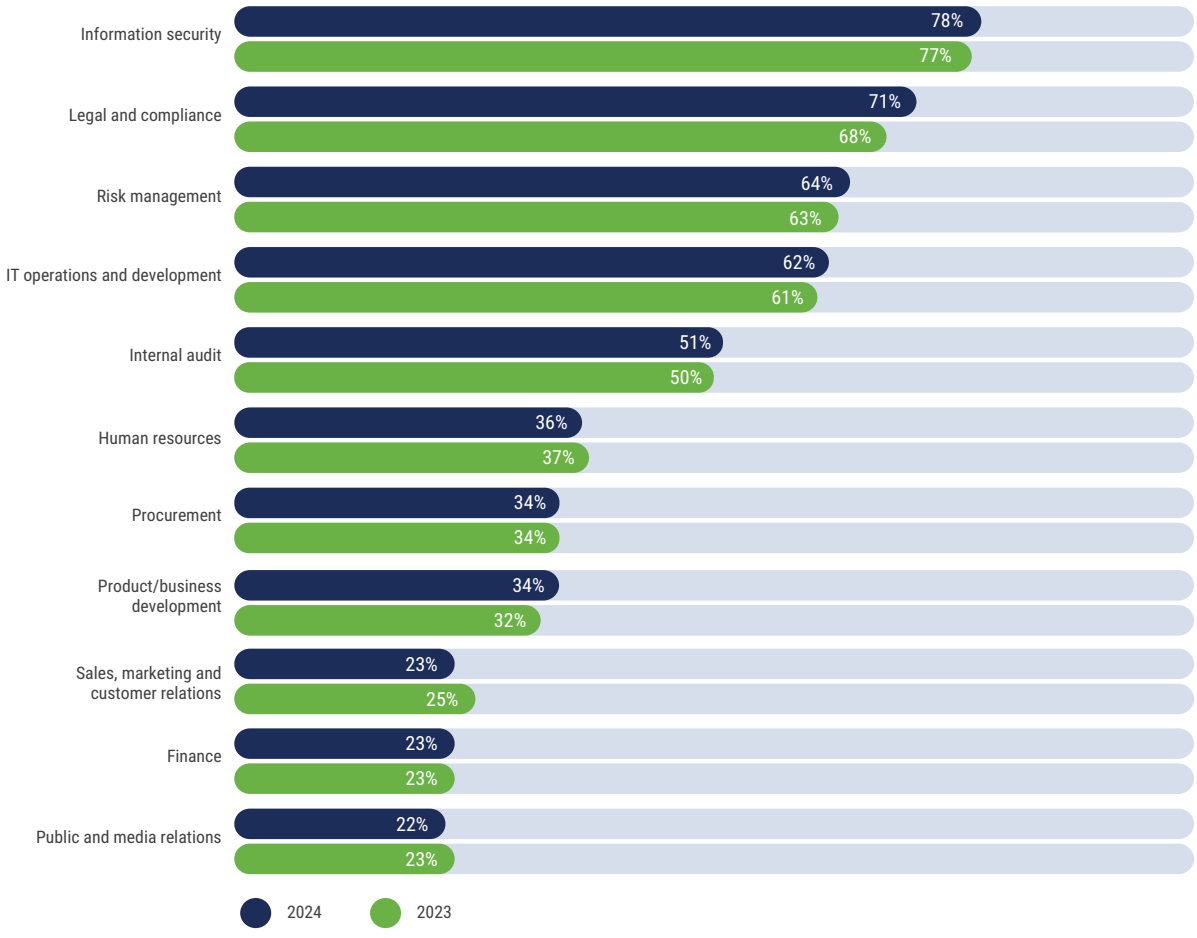
Collaboration

Privacy professionals must collaborate regularly with other enterprise functions. **Figure 9** shows the functional areas privacy professionals must work with and the percentages of respondents who said they always or frequently collaborated with these departments.

It is concerning that only 34 percent of respondents regularly worked closely with procurement; only 34 percent worked regularly with product/business development; and a mere 23 percent worked regularly with sales, marketing and customer relations. Procuring technology that has strong privacy controls built in is crucial to protecting data subjects. The technology underlying an organization's offerings must protect privacy, and without being involved with the procurement process, it is nearly impossible for privacy professionals

FIGURE 9: Privacy Professionals Working Across the Enterprise

How frequently do the privacy office/privacy professionals in your organization interact with the following areas?



to practice privacy by design. Product development may leverage deceptive privacy practices, but privacy professionals who work closely with them can guide them away from products that do not align with privacy objectives. Marketing teams often rely heavily on data to inform marketing efforts, and privacy professionals can also guide marketing teams away from deceptive privacy practices and excessive consumer tracking.

Accountability for Privacy

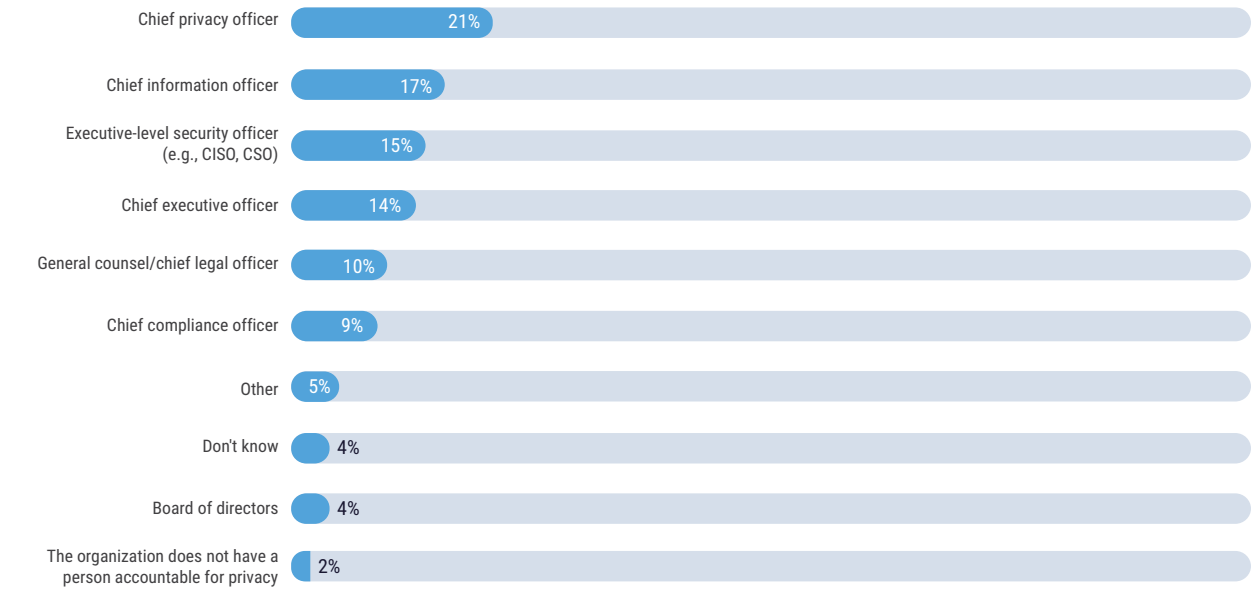
Depending on how an organization is structured and taking into account the competencies of the C-suite, privacy professionals may report to different leaders. **Figure 10** shows who is primarily accountable for privacy. These results are consistent with the 2023 survey findings.

Enterprise size may affect who is ultimately accountable for privacy. Twenty-seven percent of respondents who worked at enterprises with fewer than 250 employees said the chief executive officer (CEO) was accountable for privacy, but only 8 percent of respondents at organizations with more than 25,000 employees said the CEO was primarily responsible. Thirty-two percent of respondents at enterprises with 25,000+ employees said the chief privacy officer was primarily accountable for privacy at their organization, but only 10 percent of respondents at enterprises with fewer than 250 employees said a CPO was primarily responsible. Compared to a chief privacy officer, a CEO is likely less aware of what privacy entails and why it is important, and privacy professionals who report to the CEO could face a bigger challenge in obtaining executive-level buy-in for privacy initiatives.

Privacy professionals should be aware of potential conflicts of interest depending on where the privacy function resides within an organization. Security may be at odds with privacy at times. For example, the security concept of nonrepudiation (that is, the assurance that a party cannot later deny originating data and provision of proof of the integrity and origin of the data that can be verified by a third party) could be at odds with an individual's right to communicate privately—for example, with an anonymous ethics hotline. Additionally, reporting to legal could represent a conflict of interest because privacy focuses on the rights of individuals while legal departments focus primarily on protecting the enterprise.

FIGURE 10: Accountability for Privacy

Who is primarily accountable for privacy in your organization?



Boards of Directors and Privacy

The board of directors can have a significant impact on an enterprise's privacy program. Fifty-seven percent of respondents said their boards adequately prioritized privacy. This is a slight increase compared with last year when 55 percent of respondents said their boards adequately prioritized privacy. **Figure 11** shows board prioritization of privacy.

Boards may prioritize privacy programs in a few ways. A compliance-driven approach considers privacy a regulatory requirement. An ethical approach prioritizes privacy regardless of applicable laws and regulations. Some enterprises may view privacy protection as a competitive advantage, and many enterprises will combine approaches to privacy prioritization. **Figure 12** shows how boards view privacy programs.

Last year, only 33 percent of respondents said their boards viewed privacy as being compliance-driven, while this year that number rose to 44 percent. It is possible that recent enforcement actions and new privacy laws and regulations have made compliance a higher priority for enterprises. The compliance-driven perception was slightly higher among Europe-based respondents, with 49 percent reporting their boards viewed privacy programs as compliance-driven. This result is unsurprising, considering the far-reaching impacts of the European General Data Protection Regulation (GDPR).

Seventy-four percent of respondents said their organization's privacy strategy was aligned with organizational objectives, 11 percent said it was not and 15 percent did not know. This represents a slight increase from last year, when 73 percent of respondents said their organization's privacy strategy was aligned with organizational objectives.

FIGURE 11: Board Prioritization of Privacy

Do you believe that your board of directors has adequately prioritized privacy in your organization?

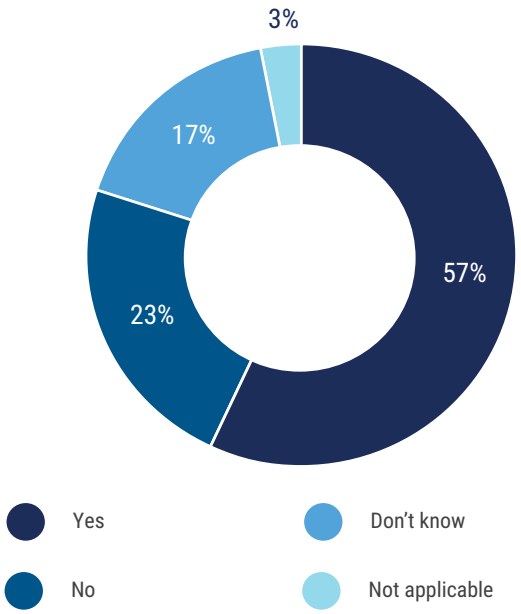
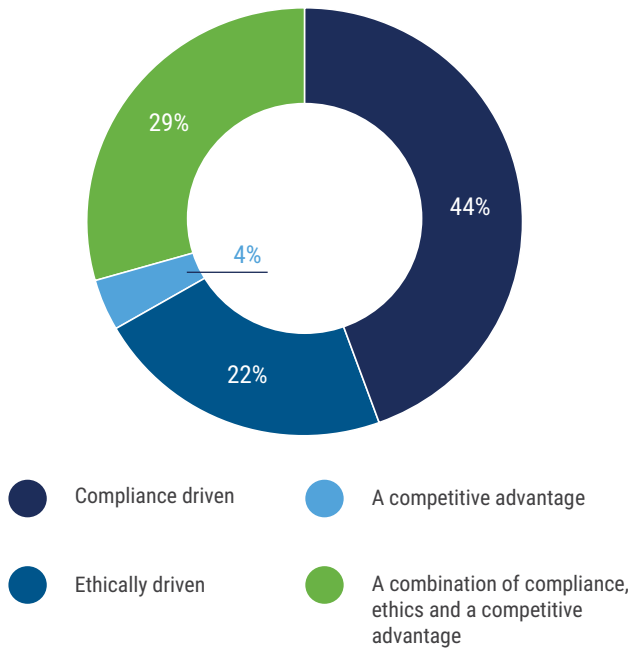


FIGURE 12: Board Perceptions of Privacy Programs

Do you think your board of directors views your enterprise's privacy program as:



Funding

Board prioritization and the organizational perception of privacy is important as it could affect staff buy-in for privacy initiatives and resources available for privacy teams. **Figure 13** shows respondents' perceptions of privacy funding at their enterprises.

This year's survey finding that 43 percent of respondents considered their organization's privacy budgets underfunded is fairly consistent with last year's, when 42 percent held that view. However, respondents were much less optimistic about the future of privacy budgets this year compared to last year (see **figure 14**).

It appears that privacy budgets have been declining significantly in recent years. Just two years ago, only 8 percent of respondents believed their privacy budgets would decline in the next 12 months. It is surprising that in the midst of a rapidly evolving regulatory landscape, privacy professionals this year still

FIGURE 13: Funding for Privacy

Do you feel your organization's privacy budget is currently:

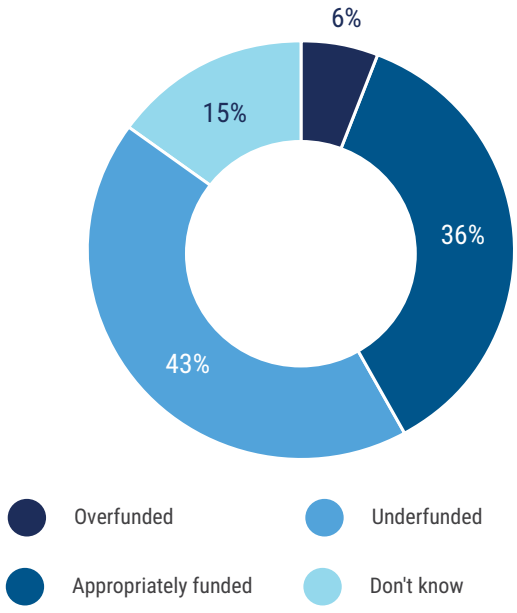
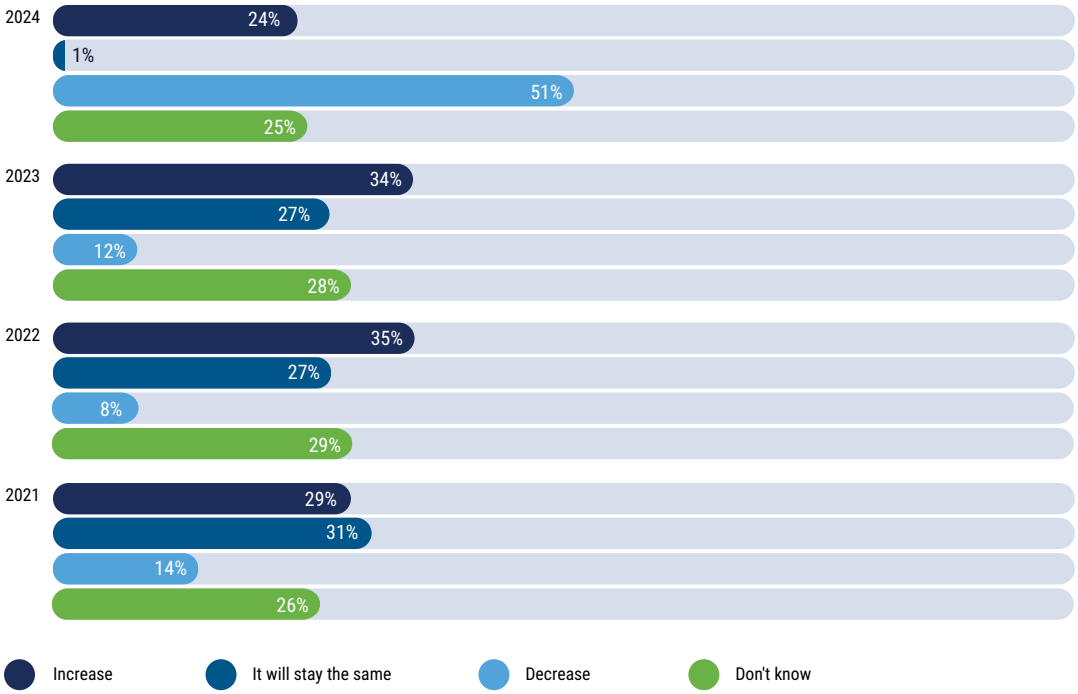


FIGURE 14: Privacy Budgets in the Next 12 Months

How will your organization's privacy budget change in the next 12 months?



believed their budgets for the next year would shrink. This is especially concerning because 63 percent of respondents who believed their privacy budgets were already underfunded anticipated that funding would decrease in the next 12 months. This suggests that some teams that are already struggling with limited resources may find their problems exacerbated next year.

Perhaps allaying some fears about budget cuts, only 5 percent of respondents expected a significant decrease compared to 46 percent who said their privacy budgets would somewhat decrease. Budget cuts may not be drastic, but privacy professionals should be prepared for some cuts. This aligns with global economic trends; global growth in 2024 is forecast to be lower than in 2023.[1]

But privacy may be disproportionately affected by the economic downturn: Only 11 percent of respondents to ISACA's *State of Cybersecurity 2023* survey anticipated a decrease in their cybersecurity budget.[2] This could be because high-profile breaches, such as the LastPass breach,[3] and concerns about ransomware have motivated enterprises to not cut cybersecurity spending. More concerning is the possibility that enterprises believe cybersecurity and privacy are interchangeable and that cybersecurity professionals are tasked with privacy and vice versa.

Artificial Intelligence

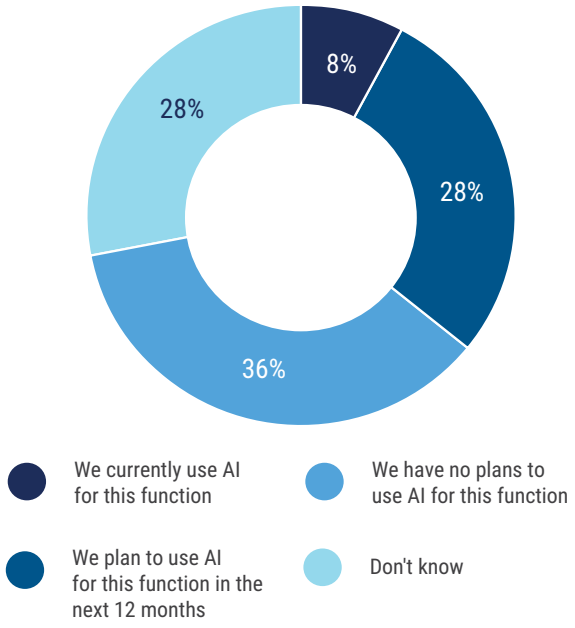
Despite challenges associated with understaffing and underfunding, most respondents were not leveraging artificial intelligence (AI) for privacy work. **Figure 15** shows a breakdown of respondents' use of AI in privacy-related tasks.

Only 8 percent of respondents were using AI for privacy-related tasks, compared with last year when 11 percent of respondents said they were using AI. In last year's survey, 20 percent of respondents said they planned to implement AI for privacy tasks in the next 12 months, but based on this year's survey findings, that has not happened.

This is surprising, as 41 percent of respondents to a recent ISACA survey indicated that their organizations' employees were using generative AI.[4] It is possible that privacy professionals are not using AI, but their colleagues across the organization are—and without any privacy-related considerations or oversight.

FIGURE 15: Plans to Use AI

What are your organization's plans to use AI (bots or machine learning) to perform any privacy-related tasks?



1 Organization for Economic Co-operation and Development (OECD), "Confronting Inflation and Low Growth," *OECD Economic Outlook, Interim Report September 2023*, https://www.oecd.org/economic-outlook/september-2023/

2 ISACA, *State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources and Cyberoperations*, USA, 2023, https://www.isaca.org/resources/reports/state-of-cybersecurity-2023

3 Winder, D.; "Why You Should Stop Using LastPass After New Hack Method Update," Forbes, 3 March 2023, https://www.forbes.com/sites/daveywinder/2023/03/03/why-you-should-stop-using-lastpass-after-new-hack-method-update/?sh=4c06e06928fc

4 ISACA, "Generative AI: The Risks, Opportunities and Outlook," 25 October 2023, https://www.isaca.org/resources/infographics/generative-ai-2023-an-isaca-pulse-poll-infographic

The reluctance to adopt AI might be a positive sign: Survey respondents might understand that AI is not a panacea for privacy challenges. Enterprises in organizations with lower revenues and smaller staff sizes were considerably less likely to use AI. Forty-eight percent of respondents in enterprises with less than US$50 million in revenue said they had no plans to use AI for privacy-related tasks, compared to just 24 percent of those in enterprises with more than US$1 billion in revenue. Forty-nine percent of respondents in enterprises with fewer than 250 employees said they had no plans to use AI for privacy-related tasks, compared to just 23 percent of those in organizations with more than 25,000 people. These findings suggest that small enterprises understand that leveraging AI requires governance and resources to effectively manage it, and employing AI for privacy-related tasks might stretch an already overtaxed staff.

Privacy professionals largely seem to understand that AI could carry privacy-related risk. For example, if an AI platform uses inputs to train future outputs, inputs of personal information could shape future outcomes, which might result in privacy violations. Forty-five percent of respondents who were not at all confident in their enterprise's data privacy abilities said they had no plans to use AI for privacy-related functions, and 53 percent of respondents who were not so confident in their data privacy abilities said they had no plans to use AI for privacy tasks. This suggests that privacy professionals understand the risk associated with AI and that until their privacy program matures, the risk associated with using AI for privacy tasks outweighs the benefits.

Compliance

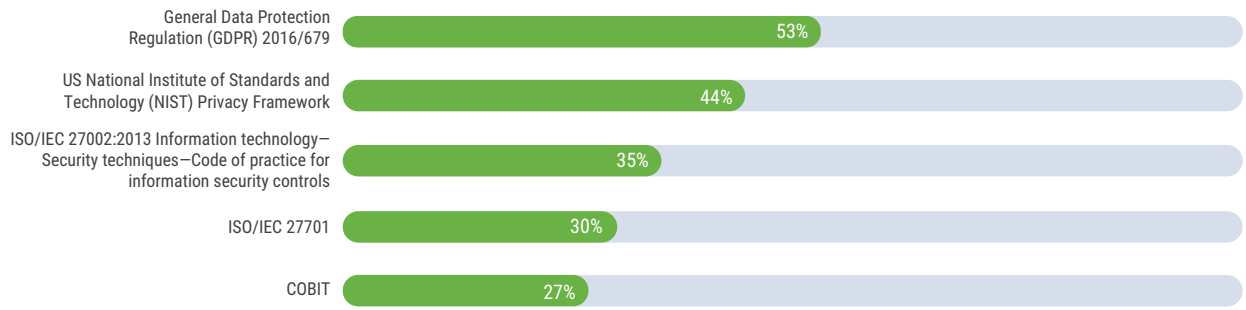
To date, more than 160 privacy laws have been enacted internationally.[5] Because of the numerous privacy laws and regulations in effect, privacy teams are often scrambling to keep up with their compliance-related obligations. Using a framework or legal foundation to manage privacy can provide enterprises with clear objectives. Seventy-eight percent of survey respondents said they used a framework or law/regulation to manage privacy in their organizations.

Figure 16 shows the five frameworks and regulations most commonly used to manage privacy.

There are some regional differences as to which frameworks or regulations are used to manage privacy. For example, 78 percent of respondents in Europe used the GDPR, and 61 percent of respondents in North America used the NIST Privacy Framework to manage privacy.

FIGURE 16: Frameworks and Regulations Used to Manage Privacy

Which frameworks/regulations are used to manage privacy in your organization?



5 Greenleaf, G.; "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills," *181 Privacy Laws and Business International Report (PLBIR)*, 1, 2-4, 3 May 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146#:~:text=The%20Tables%20which%20document%20these,the%20total%20to%20162%20globally.

Technical privacy professionals must work closely with legal/compliance teams to understand their regulatory obligations. **Figure 17** shows how often technical privacy professionals reported meeting with legal/compliance professionals.

Privacy professionals who meet with legal/compliance teams only when new privacy laws and regulations go into effect should consider meeting on a regular schedule. The challenge with meeting only when new laws and regulations go into effect is that enforcement actions or data transfer-related resources that are not new per se—for example, the EU-US Data Privacy Framework—could significantly impact an enterprise's day-to-day operations. Additionally, meeting regularly can allow technical privacy professionals to check in with legal practitioners to evaluate if the privacy controls in place do, in fact, meet the enterprise's privacy obligations.

Many enterprises are aiming higher than achieving compliance; they are putting additional privacy controls in place that go beyond what is legally required. This might include applying controls to data not subject to privacy laws or regulations—for example, adopting GDPR requirements for all data subjects regardless of their location. The top five most-used additional controls reported by survey respondents are:

- Identity and access management (74 percent)
- Encryption (73 percent)
- Data security (72 percent)
- Data loss prevention (67 percent)
- Incident response plan (63 percent)

Given the myriad privacy laws and regulations with which enterprises may need to comply, it is not surprising that some privacy professionals struggle to achieve compliance with new privacy laws and regulations and have concerns about their ability to ensure data privacy. **Figure 18** shows respondents' confidence in their ability to achieve compliance.

FIGURE 17: Frequency of Meetings Between Technical Privacy and Legal/Compliance Professionals

How often do technical privacy professionals meet with legal/compliance professionals to understand legal and regulatory requirements?

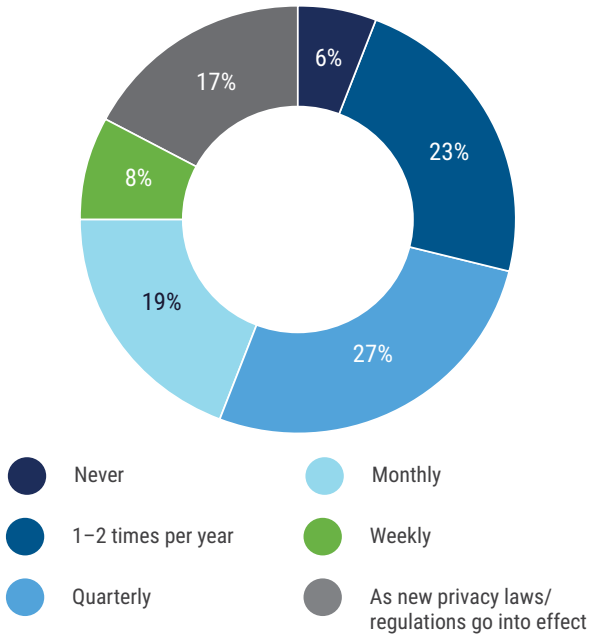
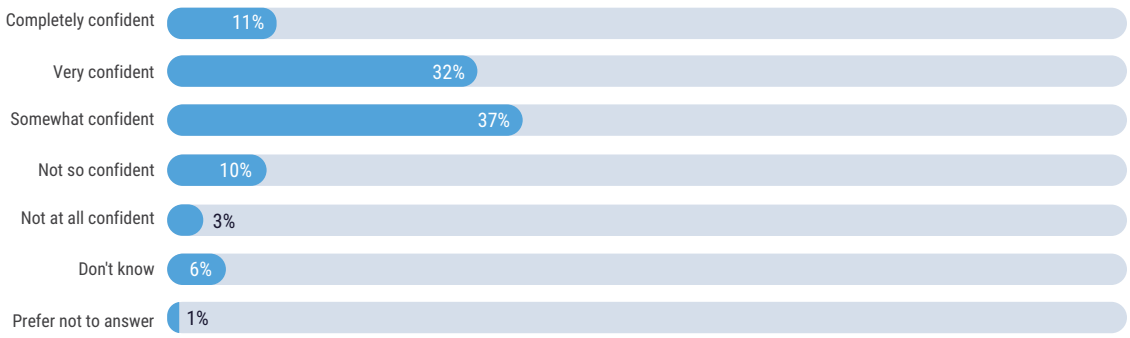


FIGURE 18: Confidence in Achieving Compliance

How confident are you in your organization's privacy team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations?



As a result of some privacy laws and regulations, data subjects may have the right to request that their data be accessed, deleted or moved. Thirty-one percent of respondents said the number of data subject requests increased in the past year, while 31 percent said it stayed the same, 6 percent said it decreased and 33 percent did not know. Although the percentage of respondents who did not know about data subject requests may seem high, many people working in technical privacy may not resolve data subject requests or work directly with customers; they may be working on the back end, ensuring that the necessary technology is in place to honor data subject requests.

Privacy by Design

Privacy by design refers to the integration of privacy into the entire engineering process. It involves thinking of privacy as part of basic functionality rather than treating it as an afterthought. It is worthwhile to regularly practice privacy by design as it could help with compliance efforts. In the event of a privacy breach, data subjects may experience less harm if the enterprise practices privacy by design. Sixty-nine percent of respondents said their enterprises practiced privacy by design when building new applications and services, while 17 percent said their enterprises did not and 14 percent did not know. **Figure 19** shows how frequently respondents practiced privacy by design.

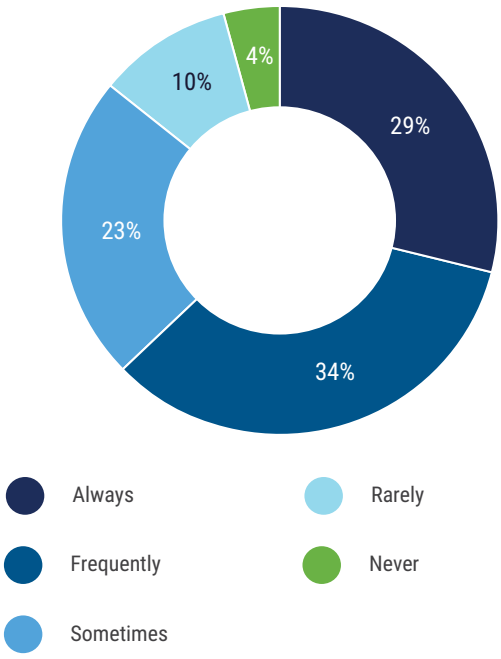
Consistent with previous years' survey results, those at enterprises that always practice privacy by design tend to have more resources. For example, the median staff size at enterprises that always practice privacy by design was 15 compared to 9 for total respondents. However, the median staff size among enterprises that always practice privacy by design was considerably lower compared with last year when the median staff size was 19.

Some other key trends among those who always practice privacy by design compared to the total respondents include:

- More likely to say their technical privacy department was appropriately staffed (42 percent vs. 34 percent total)
- More likely to believe their board of directors adequately prioritized privacy (77 percent vs. 57 percent total)
- Less likely for boards to view the privacy program as purely compliance-driven (35 percent vs. 44 percent total)

FIGURE 19: Frequency of Practicing Privacy by Design

How often does your enterprise practice privacy by design?



- More likely to feel their privacy budgets were appropriately funded (50 percent vs. 36 percent total)

Respondents who worked in enterprises that always practiced privacy by design were more likely to be completely and very confident in the ability of their organizations' privacy teams to ensure data privacy and achieve compliance with new privacy laws and regulations (71 percent vs. 43 percent total), but this may represent false confidence. Enterprises that always practice privacy by design were just as likely to have experienced a material privacy breach in the last year as the total respondents (11 percent for both). It is imperative that those practicing privacy by design understand that it does not make them immune to privacy breaches.

Privacy Awareness Training

Almost any employee can cause a privacy breach, so it is important that all staff complete privacy awareness training. The survey results reflect this belief as most survey respondents said their organizations provided privacy awareness training (86 percent). **Figure 20** shows how frequently respondents' organizations provided privacy awareness training. These findings are comparable to last year's results.

While it is slightly concerning that 9 percent of respondents said no privacy awareness training was conducted, it is possible those respondents were independent consultants or operated a small privacy consulting business comprised entirely of privacy experts. That said, even very small organizations should ensure that all employees receive some kind of privacy training on a regular basis. Most respondents (71 percent) said privacy awareness training had a positive impact on privacy awareness in their organizations.

Providing the same training year after year will not provide value for employees who have already completed it in prior years. It is worthwhile reviewing and revising privacy training on a regular cadence to ensure it is up-to-date and provides meaningful information to staff. **Figure 21** shows how frequently enterprises provided privacy awareness training.

Nearly half of respondents (49 percent) pointed to a lack of training or poor training as a common privacy failure. Part of reviewing privacy awareness training should be evaluating its effectiveness. Privacy teams should select metrics to evaluate training effectiveness and track trends over time.

FIGURE 20: Frequency of Privacy Awareness Training

When does your organization provide privacy training?

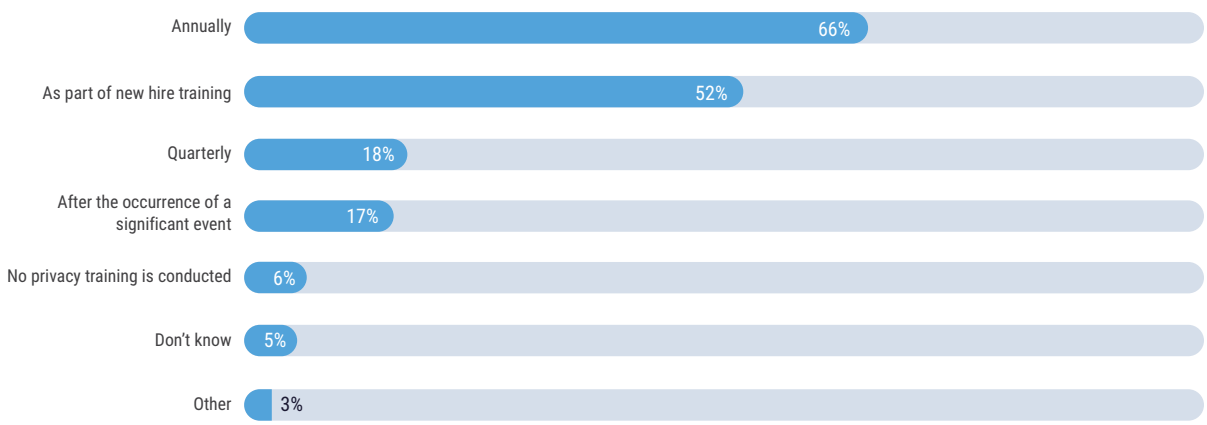
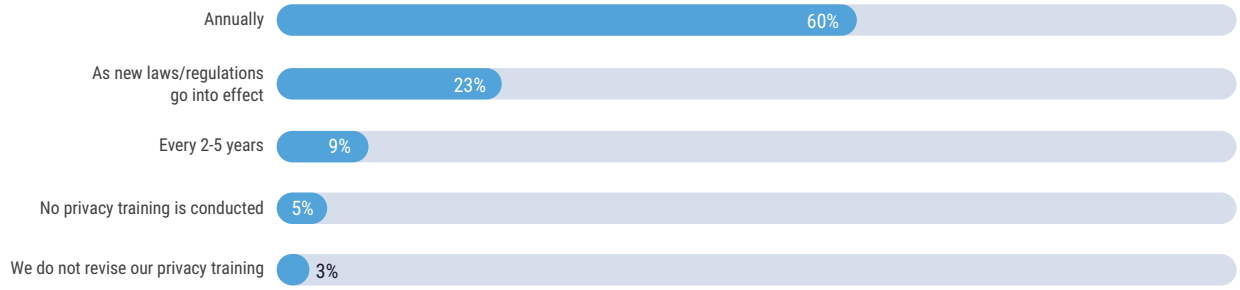


FIGURE 21: Reviewing and Revising Privacy Awareness Training

How often does your organization review and revise privacy awareness training?



The metrics respondents used to evaluate their privacy training programs include:

- Number of employees who completed privacy training: 65 percent
- Number of privacy incidents: 56 percent
- Number of privacy complaints received from customers: 37 percent
- Comparison of pre-and post-training assessments: 23 percent

Enterprises should be wary of relying solely on the number of privacy incidents and/or complaints to measure the quality of privacy training. These measures are reactive; they indicate that an incident has occurred or a customer has experienced a privacy harm. The damage has been done, and revising privacy training after the fact likely will not restore consumer trust. While tracking the number of employees who have completed privacy awareness training can be valuable, it does not provide any insight into whether employees have learned anything, if they found the training useful, or if they became more capable of acting in ways that align with privacy objectives. Pre- and post-training assessments—even just a few true/false questions asked before and after the training—may provide better insights on the quality of privacy training.

Enterprises should be wary of relying solely on the number of privacy incidents and/or complaints to measure the quality of privacy training. These measures are reactive; they indicate that an incident has occurred or a customer has experienced a privacy harm. The damage has been done, and revising privacy training after the fact likely will not restore consumer trust.

In some enterprises, privacy awareness training and security awareness training are not separated. While that is not necessarily a problem, it is possible that some enterprises consider privacy and security to be interchangeable. It is important that if the two are combined, both privacy- and security-specific information is included. Sixty percent of respondents separated privacy awareness training from security training; 29 percent did not separate them; and 6 percent did not know if they were separated. (Five percent of respondents' organizations did not offer privacy awareness training.)

Privacy Breaches

Respondents' reports of privacy breaches were consistent with last year's survey findings. As in 2023's report, 11 percent of respondents in this year's survey said their organizations experienced a material privacy breach in the last 12 months. Sixty-three percent said their organizations did not, 8 percent preferred not to answer, and 18 percent did not know. The large percentage of respondents who did not know if their enterprises experienced a privacy breach signals a broader issue about breach response and data classification. Some organizations may know they experienced a breach but not know if personal information was compromised, which may mean data classification efforts need improvement.

Figure 22 shows respondents' perception of breaches this year compared with last year. Although the percentage of respondents' organizations that experienced a breach is the same as last year, only 18 percent of this year's respondents felt they were experiencing the same number of breaches as last year.

There was no consensus among respondents on the likelihood of experiencing a material privacy breach in the next year, as shown in **figure 23**. It is concerning that almost a quarter of respondents did not know the likelihood of experiencing a privacy breach. This may indicate that privacy risk is an area of growth for many enterprises, and it could also indicate that privacy professionals need a better definition of what constitutes a privacy breach.

FIGURE 22: Comparing Breach Trends

Is your organization experiencing an increase or decrease in material privacy breaches as compared to a year ago?

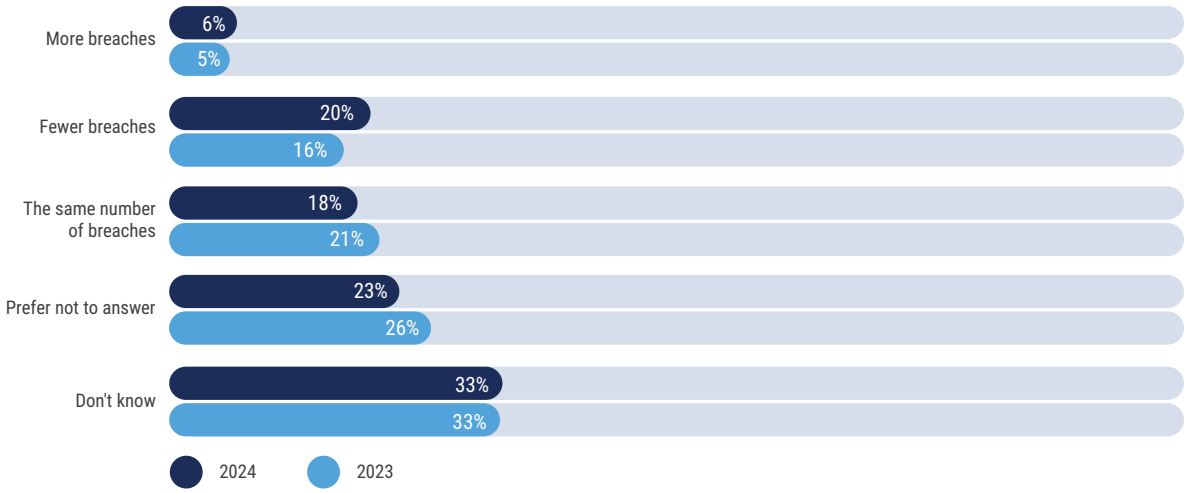
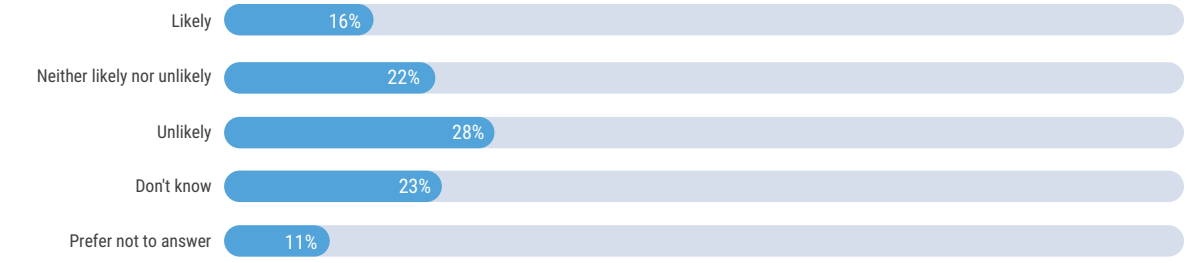


FIGURE 23: Likelihood of a Privacy Breach in the Next Year

How likely is it that your organization will experience a material privacy breach next year?



Conclusion

Privacy laws and regulations have required many enterprises to prioritize privacy and expand their privacy-related functions. Consumers have become more focused on privacy, and many enterprises believe that their customers will not patronize them if their data is not properly protected.[6] Enterprises that do not protect data are at risk of losing trust with their consumers, as privacy violations can result in heavy fines and reputation-damaging headlines.

Although many privacy teams work with limited resources, the ISACA survey reveals good news: Enterprises are not experiencing more breaches than in the past. Still, privacy teams are smaller this year than last year; considering anticipated budget cuts, privacy professionals who already feel their programs are underfunded are likely to experience more budgetary challenges in 2024. Despite these budget cuts, privacy professionals who maximize the impact of privacy initiatives can meet their privacy objectives.

6 CISCO, *Privacy's Growing Importance and Impact*, 2023, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2023.pdf?CCID=cc000160&DTID=esootr000515&OID=rptsc030828

Acknowledgments

ISACA would like to recognize:

Board of Directors

John De Santis, Chair

Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Brennan P. Baybeck, Vice-Chair

CISA, CISM, CRISC, CISSP

Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Stephen Gilfus

Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Niel Harper

CISA, CRISC, CDPSE, CISSP, NACD.DC

Former Chief Information Security Officer, United Nations Office for Project Services (UNOPS), USA

Gabriela Hernandez-Cardoso

NACD.DC

Independent Board Member, Mexico

Jason Lau

CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP

Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo

Independent Director, Former Chief Executive Officer and Executive Director, VADS Berhad Telekom, Malaysia

Maureen O'Connell

NACD.DC

Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Erik Prusch

Chief Executive Officer, ISACA, USA

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P

Chief Executive Officer, introSight Ltd., Israel

Pamela Nigro

ISACA Board Chair 2022-2023

CISA, CGEIT, CRISC, CDPSE, CRMA

Vice President, Security, Medecision, USA

Gregory Touhill

ISACA Board Chair 2021-2022

CISM, CISSP

Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021

Former Chief Risk Officer, Hudson City Bancorp, USA

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *Privacy in Practice 2024* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/