# IAPP-EY Annual Privacy Governance Report 2015

iapp

EY

Building a better working world

# Introduction

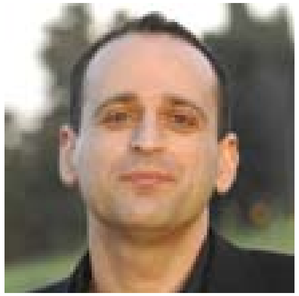
For those of us long in the thick of it, privacy can sometimes seem age-old. *Privacy & Freedom*, Alan Westin's seminal text on digital privacy, will celebrate its 50th anniversary in 2017. The global data protection authorities are coming together for their 37th annual conference in October. The International Association of Privacy Professionals will hit 25,000 members before 2015 is out.

However, if there is one thing made clear by this first in a series of annual EY-IAPP Privacy Governance Reports, it is that privacy governance in organizations is still nascent. Just under a quarter of the nearly 800 respondents to our survey were the creators of the privacy program at their organization. And only 36 percent of those heading up privacy programs have privacy as their sole occupation. This is not one of those industries where old warhorses wax poetic about the good old days before the Internet changed everything.

Yes, privacy is young. Some would say it is adolescent. But with adolescence come growing pains. We know that companies continue to struggle with where to sit privacy in the organization, how to integrate privacy into operations, how to ensure "privacy by design" or "privacy by default." Who should the privacy officer report to? What should her title be? Should she focus on complying with laws or on strategizing data utilization? Some of you may even feel like you're making it up as you go along.

That's why EY and the IAPP decided to join forces to uncover the common and leading practices in the field today. This data is a stake in the ground, marking how far data privacy practices have come and how far they have yet to go.

**J. Trevor Hughes**
*CIPP, CEO and President, IAPP*



***Sagi Leizerov***
*CIPP/US, Executive Director, Privacy Practice, EY*

*The study was sponsored by EY. All copyrights remain those of the IAPP and the IAPP retained all editorial oversight.*

The data will also allow organizations and the privacy professionals who govern data inside them to benchmark themselves against emerging industry standards around how privacy is implemented in day-to-day activities. One of the best things about working in privacy is that hardly anyone can argue that "this is how we've always done it." But that also can make the work of privacy particularly difficult. What's normal? Or, to put it in regulatory parlance, what's *reasonable*? Which practices can help an organization demonstrate accountability for the personal information they process?

As privacy rapidly evolves alongside technologies and business practices that are fueled by data consumption, this annual governance survey and report can help serve as a guidepost for privacy programs as they evolve and mature. To that end, too, we hope that you will let us know which aspects of privacy programs we should explore further, which questions you'd like answered, what new areas to develop more. We want to provide you with data and case studies that help your organization do the job of privacy better.

This report is just a start. Like the work of privacy itself, it will continue to grow and expand in future years. Before putting our heads down and getting back to the nitty gritty of privacy and data governance, it's good to take a close look at what others are doing.

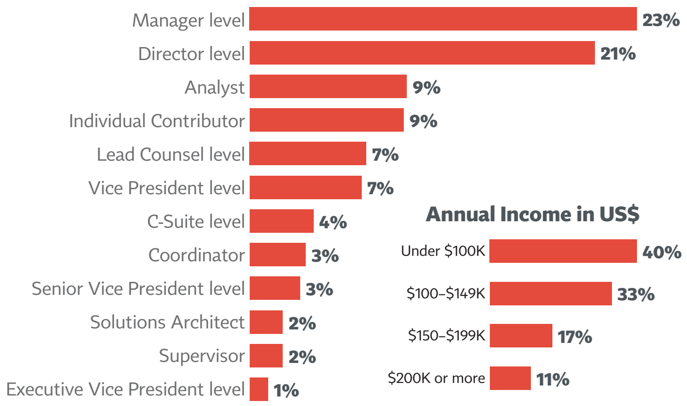
# Executive Summary

Privacy programs don't just happen. They are created and governed by privacy professionals the world over and it may well be that no two are the same. But what does the average privacy program look like? In the spring of 2015, the IAPP and EY endeavored to find out, fielding an in-depth survey returned by nearly 800 privacy professionals. Where does privacy sit in the organization? How many team members are there? With whom does the privacy team most often work? What are the team's priorities? How does a privacy team evolve as it matures? What are the hallmarks of a mature privacy program?

The following report has the answers to these questions and more.

What's clear is that privacy is a thriving industry in rapid growth. Still nascent, it already employs thousands of professionals with diverse backgrounds active across a broad range of organizational structures, from tech start ups through regulated banks and health care providers to government agencies, in the United States, Europe and around the world. Privacy professionals earn well, are trained in law, business and technology, influence a broad swath of departments across their organizations and are increasingly part of strategic management teams. At the same time, privacy programs clamor for additional resources and seek more sophisticated and efficient technological tools to monitor, manage and protect data flows in their organizations.

Level in Company



Annual Income in US$

The data reveal several important trends:

- Privacy professionals are well paid, with almost a third earning more than $150,000 a year, and take part in a rapidly growing industry. They expect their staff and budgets to grow over the next year, and report a growth in their influence within their organizations. They interact closely with all parts of their companies, particularly information security and IT, legal and regulatory compliance and HR, and to a lesser extent product teams, marketing and PR. Privacy typically belongs to the legal department, with information security and IT a distant second. Increasingly, the leading privacy role, typically a Chief Privacy Officer, is equivalent in seniority to the longer established Chief Information Security Officer.

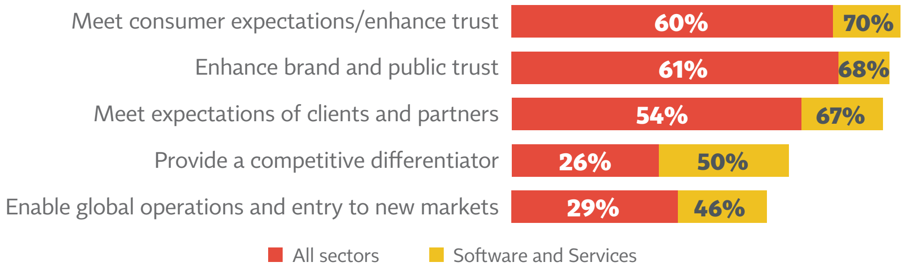
*Unregulated industries*, such as online, software and retail, report a greater investment in privacy programs as well as a more strategic focus on risk mitigation, brand management and consumer expectations. In addition, unregulated businesses are more focused than average on global expansion and positioning privacy as a competitive differentiator. Privacy teams at software and services firms in particular exert far greater influence over product managers, product engineers and product designers than general industry numbers.

*Regulated industries*, such as banking and healthcare, place greater focus on compliance and accountability processes, including internal audits, privacy impact assessments and vendor-management programs. In addition, regulated industries report a greater tendency to create privacy working groups, comprising senior officers from across the organization. *Government* programs report low budgets and staff shortages and a focus on compliance and prevention of data loss. Government privacy officers regularly deploy privacy impact assessments and interact with records management departments.

- There is a close correlation between the *maturity of privacy programs* and *company size*. The privacy programs in large companies are far better staffed (24 professionals on average) and resourced ($1 million on average) than those in small and medium enterprises (two and $75,000 respectively). In addition, fewer privacy professionals in large companies report being engaged in non-privacy activities. The more mature a privacy program the more it is likely to be risk-based as opposed to focused on compliance. Mature programs employ a plethora of technical, organizational and legal privacy solutions, including hiring external counsel, creating privacy working groups, undergoing privacy audits, administering vendor-management programs and performing privacy impact assessments. In addition, mature programs are routinely involved in data-related projects at an early stage and on an ongoing basis.

You might expect that given their emphasis on strategic risk mitigation and brand management, privacy programs in unregulated companies are, on average, more mature. But this does not pan out, as the numbers show a similar maturity curve across industry segments and the private/public sector divide. This demonstrates further that privacy is still a nascent industry, which emerged across sectors at approximately the same time frame.[1]

**Main Reasons for Privacy Program**



- Of those *companies operating in Europe*, privacy programs tend to cluster around the mid-maturity stage. American-based programs are significantly larger than those in Europe in terms of both budgets and staffing, and U.S.-based teams expect their programs to grow more than their European peers. For the European professionals, increasing consumer trust is a high priority. Reflecting a more compliance-oriented focus, privacy professionals in the EU would like to have more say in the workings of a whole range of departments, including information security and IT, corporate ethics, HR, and product managers, designers and engineers.

These are just the top-level insights provided by the analysis and data within this inaugural 2015 Privacy Governance Report, conducted by the IAPP and EY. As the average privacy program is just seven years old, we can expect these programs to continue to evolve considerably.

[1] Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 Ohio St. L. J. 897 (2013).

# Contents

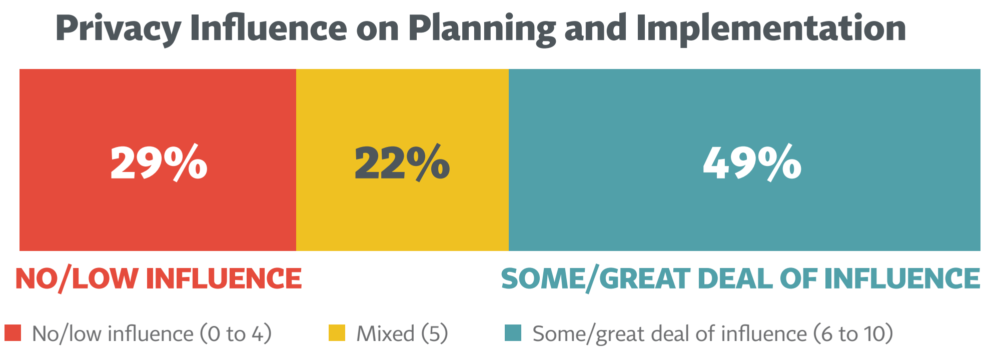
# 1 How the Job of Privacy Is Done

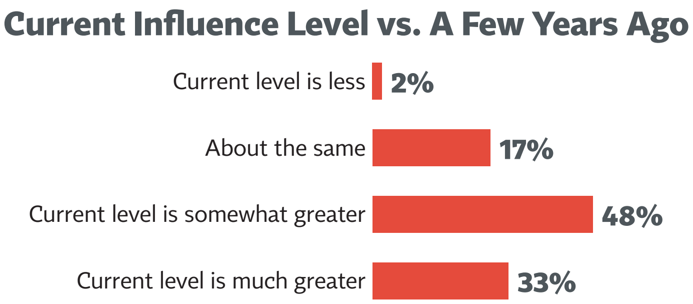
- How the Job of Privacy Is Done
- Organizational Setup
- Privacy v. Security? Privacy and security
- Proactive v. Reactive
- Tools and Resources
- How Regulation Affects Operations
- Unregulated Industries
- Regulated Industries
- Organizational Size and Maturing Operations
- Large ≠ Mature
- Region
- Conclusion

## How the Job of Privacy Is Done

While still a relatively nascent profession, the data shows privacy is a good industry to work in and is geared to continue to grow for the foreseeable future. Some 60 percent of privacy professionals earn six-figure salaries, with 28 percent making more than $150,000 a year. Fifteen percent of respondents are at the VP level or higher in their firms, with four percent in the c-suite and 44 percent at the manager or director level. About a third of respondents predict their budget will grow next year; half expect it to remain the same, compared to just six percent who expect it to shrink.

We can expect demand for privacy professionals to be high in 2016 and beyond, with salaries on the rise





**CASE STUDY: Training the Business for Success**

"Utopian privacy doesn't exist," said **Mark Keddie, Chief Privacy Officer at BT Group** (formally known as British Telecom). "I came to understand that years ago."

So, when he came to BT nearly four years ago after heading up a team at British Petroleum (BP), he brought a risk-based approach with him. Immediately, he found a lot of risk was being created simply because privacy was perceived as being low down the list of considerations during the product and service design.

"The culture was so commercially focused that, perhaps understandably, privacy wasn't recognized as being a day zero issue," Keddie said. "Now, we've turned a massive corner where people actually understand what the value of privacy is to our customers and the BT brand, beyond 'it's a nice to have'."

That didn't happen by accident. Keddie, who reports to the Chief Compliance Officer up through the General Counsel to the CEO, installed a rigorous training program to educate everyone at BT in both product development, and those who touch data more generally.

"By educating our technical and commercial culture," Keddie said, "we've made a massive step change in our wider organization, and you see the fruits of that as people now come to us of their own free will … One of our commercial-facing chief executives, with a reputation for a razor-like business acumen, recently spoke about the importance of achieving

***continued on 4***

and positions filled that are of increasing importance to the organization.

This rapid growth of the profession has recently been reflected in membership figures for the IAPP. It took the organization more than 10 years to amass its first 10,000 members, compared to just two years for the next 10,000 to join. The ranks of the organization currently number more than 23,000 members in nearly 90 countries around the globe.

With data breaches rampant[1] and privacy snafus regularly making front page headlines in the *Wall Street Journal* and *New York Times*,[2] senior management and boards of directors have come to recognize that privacy is a considerable risk to the bottom line, affecting brand, reputation, trust and consumer expectations. The influence of privacy pros in their organizations is growing, with 73 percent responding that their level of influence is somewhat greater or much greater than in past years. Similarly, about half of the respondents state that the privacy function of their company is integrated into the planning and implementation of initiatives that involve personal information, with a staggering 81 percent reporting an increase in the degree of integration over the past few years.

[1] *See, e.g.*, David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers*, NY Times, June 4, 2015, http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html; Dino Grandoni, *Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions*, NY Times, July 20, 2015, http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html.

[2] *See, e.g.*, Wall Street Journal, *What They Know Series*, WSJ, 2012, http://www.wsj.com/public/page/what-they-know-digital-privacy.html; Reed Albergotti, *Furor Erupts Over Facebook's Experiment on Users*, WSJ, June 30, 2014, http://www.wsj.com/articles/furor-erupts-over-facebook-experiment-on-users-1404085840; Charles Duhigg, *How Companies Learn Your Secrets*, NY Times, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

***continued from 3***

a wider culture of privacy beyond security alone. That's a great message to give our people and a huge achievement in terms of embedding the right values around privacy in a demanding commercial environment."

The second-most common activity that privacy pros engage in, training is on the list of responsibilities for 78 percent of working professionals, but for Keddie's team of 26, it's near enough 100 percent.

"I do make it a condition of people on my team that they have to be comfortable leading training," he said. "And if they're not comfortable, then they learn to present; they get a mentor on the team to teach them to present. Privacy needs to have a human face in the organization—not just an intranet address."

By nature, however, those who get into privacy tend to be pretty good trainers, Keddie has found. "The nature of privacy can be pretty complicated in comparison to other binary compliance issues such as bribery and corruption. Sometimes when you're talking about privacy, it's shades of grey." Having to constantly navigate thorny issues makes privacy professionals good at talking through the challenges that people throughout the company are encountering.

**"By educating our technical and commercial culture," Keddie said, "we've made a massive step change in our wider organization."**

Keddie also believes it's important to have the training be specific to the job each employee is doing. "We have mandatory role-based training,"

***continued on 5***

Surprisingly, privacy professionals remain more optimistic about opportunities for career growth in other parts of the organization than in the privacy department. More than 8 in 10 respondents agree that strong privacy experience helps open doors in the marketplace overall. This suggests that despite recent gains, privacy remains a new organizational function short on staff and resources and with great upside potential.

### Top Functional Areas Privacy Works With

| | |
|---|---|
| Information Security | 83% |
| Legal | 79% |
| Information Technology | 72% |
| Regulatory Compliance | 64% |
| Human Resources | 56% |

Privacy pros have touchpoints all across their organizations, with almost 80 percent reporting joint work with information security and IT, 80 percent with legal and regulatory compliance and 56 percent with HR. Other departments engaged by privacy professionals include product, marketing, records management, internal audit and PR. Being exposed to different parts of their organizations, privacy professionals benefit from career opportunities beyond the privacy office.

What kind of expertise does a privacy pro need to have in order to deal with a plethora of functions and specialists? In an article published in an Oxford University Press journal in 2014, University of Tilburg scholar Eric Lachaud argues that the IAPP's certification scheme is best suited to address these multilayered job requirements.[3] In fact, the

[3] Eric Lachaud, *Should the DPO be Certified?*, 4(3) Int'l Data Privacy L. 189, 198 (2014), stating, "Brought together, the schemes proposed by the IAPP are those that best fit the requirements of the GDPR concerning DPOs."

***continued from 4***

he said, "which people do once a year. That's a shift from a one-size-fits-all privacy training, which tended to have an underlying security theme.  Now, we have scenario-based training for people in the contact center, for lawyers, for IT architects, for product development teams, all designed to give awareness around the role they do. If it's just generic privacy, it's of questionable value. You'll get the marketing teams saying, 'I don't care unless it's about consent and collecting data,' and you lose them before you get to the meat of it."

Nor can you get away with sleeping through the class. The training is followed by a test of retention, which incorporates a number of question sets so employees can't simply fail until they learn the questions. "If you fail it two times, you'll come to our attention for remedial action," Keddie noted.

Example of UK Contact Center Advisor question:

**Customer service advisor Stephen takes a call from a BT customer who is requesting a copy of all the data that BT holds on them. Stephen advises that the only data BT is obliged to provide are copy bills and asks the customer if they would like Stephen to order them.**

**Q: Was Stephen correct in saying that customers are only entitled to obtain copy bills? (Y/N)**

*A: No. Some customers (individuals, sole traders and some partnerships) are entitled to obtain a copy of the personal data that BT holds on them, this is known as 'Data Subject Access Request' (DSAR) and BT may be entitled to charge a fee to process*

***continued on 6***

data demonstrates that among the credentials and degrees held by privacy professionals, IAPP certifications are by far the leading designations. Fifty-five percent of respondents hold CIPPs, 12 percent CIPMs and 10 percent CIPTs, with other non-IAPP designations, such as CISSP, CISM and CISA following suit. Privacy practices in the U.S. are more likely to have certified decision-makers than their counterparts in the EU, with certification far more prevalent in large companies and mature privacy programs.

In addition to professional certifications, privacy programs have begun to sprout in legal and non-legal academia. Santa Clara Law is offering a Privacy Law Certificate; Carnegie Mellon University a Master of Science in Information Technology–Privacy Engineering; University of Maine School of Law an Information Privacy Summer Institute. The Free University of Brussels hosts the Brussels Privacy Hub, an International Academic Privacy Research Center. As the field matures, additional law, business and technology schools can be expected to join the ranks by creating dedicated privacy programs and curricula.

## Organizational Setup

Privacy is more likely to be housed within the legal department than in any other functional area. Seventy percent of privacy programs are situated in legal or compliance departments, with 28 percent in information security or IT.  Two-thirds of professionals believe privacy is placed in the right department in the organization, with a majority of those who think otherwise pointing to legal or compliance as the appropriate setup. Accordingly, the largest plurality of privacy teams reports to the general counsel (27 percent), with the CEO and Executive Committee next (24 percent) and compliance or ethics officer third (16 percent).

***continued from 5***

*such a request. As well as copy bills, BT could have to supply copies of account notes, fault reports, emails, contracts, etc. Other business customers and corporates do not have similar rights to access to their account data so it would be a business decision whether BT responds to a request from such a customer.*

*Hint: Ensure you are aware of the DSAR process and how customers can obtain copies of their account records. (link to process for Advisors)*

Example of HR question:

**Mike is a HR Business Partner and is holding data relating to ex-employees, that left BT some time ago. As they are ex-employees Mike feels he can now delete this data.**

**Q: Is Mike correct to believe he can delete this data? (Y/N)**

*A: No. You should always establish the reason why data is being retained. Data can be retained for legal reasons, to fulfill financial obligations or for legitimate business purposes. The Information Retention Policy and Schedule details the periods for which information needs to be retained and this should be checked before any data is deleted if you are in any doubt about the retention period of specific data.*

**It's useful to listen to people and ask about what kind of issues they're encountering.**

*Hint: Always ensure that you retain data in accordance*

***continued on 7***

The responsibilities of privacy professionals are manifold, with regulatory compliance still being cited by more than 90 percent of respondents. Reducing the risk of data security breaches, (73 percent), enhancing brand, trust and consumer expectations (60 percent) and being good corporate citizens (45 percent) follow suit. Drilling in a bit deeper, professionals report they engage in many different activities, including the creation of privacy policies, procedures and governance, company privacy-related awareness and training, incident response, privacy-related communications and investigations, vendor management, privacy audits, internal privacy-related legal counsel and data inventory and mapping.

About half of respondents report their company has a privacy working group. More prevalent in large companies and mature programs, privacy working groups comprise representatives of primarily legal, information security, IT, regulatory compliance and HR departments. Less frequently, companies report privacy working groups have representatives from internal audit, corporate ethics, marketing, finance and accounting, product managers and government affairs.

**The responsibilities of privacy professionals are manifold, with regulatory compliance still being cited by more than 90 percent of respondents.**

In its recent proposal of a Consumer Privacy Bill of Rights, the White House introduced a new governance organ, Privacy Review Boards, intended to vet cases of non-contextual data use by businesses. These institutions could possibly draw on the existing expertise and infrastructure of the privacy working groups reported in this survey.

***continued from 6***

*with the Information Retention Policy and Schedule. (link to policy)*

There is also a secondary level of training for those in more high-risk groups.

The privacy team further builds targeted training sessions into the broader education program at BT in order to keep people up to speed on specific developing issues, like the new Russian data-localization law, or the pending General Data Protection Regulation.

“It’s useful to listen to people and ask about what kind of issues they’re encountering,” Keddie said. “Do they want to hear something specific? Is there a theme that’s coming up over and over again? It’s a great service to provide, but also extremely time hungry and resource demanding.”

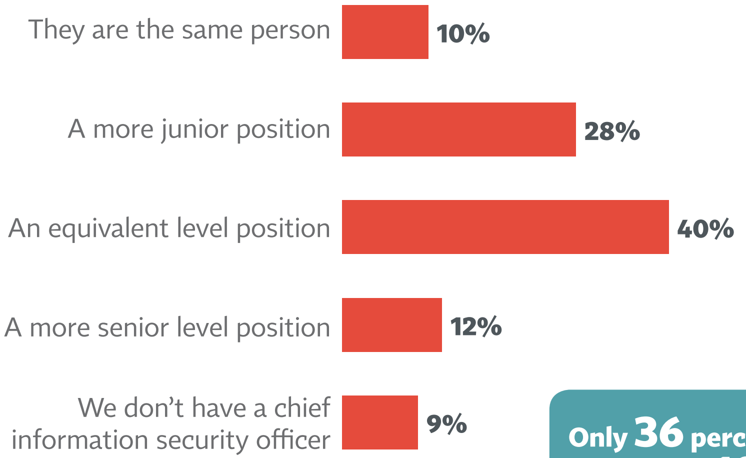
It’s worth it to reduce risk down the line, however. “We’ve spent a lot of time educating our engineers and solution architects,” he said by way of example, “around what privacy is, everything from those who want to get into the nuts and bolts of the law to those just wanting a broad understanding of context. Now, we’re getting to provide input on day zero, rather than getting that phone call on Friday that a product is going live on Monday, and can you please take a look.”

Instead, each line of business has a governance board, on which one of Keddie’s DPOs sits, through which all new products and services get discussed. “We’re being brought in a year out from deployment in some instances, with project managers and designers saying, ‘We really need you guys on board to understand our risk profile.’”

## Privacy vs. Security? Privacy *and* Security

Sometimes confused with privacy, at other times competing with it for organizational resources, information security predates privacy as a professional field and discipline. It is therefore interesting that 40 percent of respondents state that in their organizations the Chief Information Security Officer (CISO) is an equivalent-level position to the privacy lead; in 10 percent of the cases they are the same person. Otherwise, by a small margin, CISOs remain more senior than privacy leads. A clear maturity curve emerges from the data, with the CPO and CISO most likely to be the same person in smaller companies; and the CPO achieving equivalent

**Compared to Chief Information Security Officer, Privacy Lead is . . .**



**Only 36 percent of privacy leads are dedicated 100 percent to privacy**

## CASE STUDY: Roles and Responsibilities of the Privacy Team

**ADP Global Chief Privacy Officer John Gevertz** has had a long time to consider the way he'd like his privacy team to operate. He's been with the global human capital management giant, which has more than 600,000 clients around the world, for nearly 20 years.

Gevertz came into the company as an intellectual property lawyer, then built out the infosecurity legal program and then five years ago was tasked with building a global privacy operation. "We have a pretty comprehensive program now," Gevertz said of what ADP has built, and privacy is now a focus of ADP's board and executive committee.

Yes, he now feels ready this year to apply for binding corporate rules in the EU, as both a processor and controller.

**It took a while to get the attention I now have from my board and executive committee.**

That takes accountability, and that means having the right people in the right roles, with buy-in from top leadership, all of which Gevertz says is now in place, or is falling into place as we speak.

Because of his security background, and the close connection between privacy and data protection, the privacy office is closely aligned with both ADP's Global Security Organization and its legal department. While Gevertz reports to the legal department, he is a member of the security leadership team, as well.

***continued on 9***

seniority to that of the CISO as companies grow and privacy programs mature (25 percent of early stage programs, 40 percent middle stage and 48 percent mature).

Increasingly, information security professionals recognize the strategic importance and unique aspects of privacy governance. Over the past two years, the IAPP has teamed up with the Cloud Security Alliance to create Privacy. Security.Risk, a West Coast conference focused on privacy and data security. The RSA Conference, the central annual meeting place for information security professionals around the world, is now devoting an entire track to privacy. And policy initiatives in the field of cybersecurity, such as the NIST Cybersecurity Framework, devote significant attention and space to addressing privacy concerns.[4] In his January 2015 speech on the topic, President Barack Obama recognized the convergence of the two issues, saying, "if we keep on working on them together, and focus on concrete and pragmatic steps that we can take to boost our cybersecurity and our privacy, I'm confident that both our privacy will be more secure and our information, our networks, public health, public safety will be more secure."[5]

## Proactive vs. Reactive

A clear distinction arises between proactive privacy practices and ones that are more reactive and compliance-focused. Proactive programs are involved in projects from the development stage, are consulted on an ongoing basis throughout the business activity, and are integrated into

[4] *See* Get Ahead of Cybercrime: EY's Global Information Security Survey 2014, October 2014, http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf.

[5] Remarks by the President at the National Cybersecurity Communications Integration Center, Arlington, Virginia, January 13, 2015, https://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent.

***continued from 8***

Security is somewhat unique in ADP, as it is a completely converged program, covering physical, cyber, investigations and business resiliency, reporting to the chief financial officer. This emphasizes security's importance in the organization and is unlike some other organizations where security gets buried within IT or Facilities and doesn't have visibility up into the C-suite.

Similarly, ADP wants to emphasize privacy's priority. "I'm doing data flow mapping across the enterprise, cookie compliance across the enterprise," said Gevertz. "I have a public-facing role, just like our chief security officer. I'm working with clients, industry organizations. It's an outwardly facing leadership role."

Further, that close relationship with security is vital for privacy. "So much of what we do is data protection," Gevertz said, "so I need to be close to them. Security at ADP is about protecting data, money and people. When you look at it that way, they need to be able to do things such as data loss prevention. They need me and my team to facilitate that."

In fact, one privacy-trained lawyer is focused on investigations, managed through the security organization, which handles issues as diverse as cybersecurity, business resiliency and operational risk management.

It's an example of the way that the privacy team is "matrixed" throughout the organization. Here's how Gevertz's team, which is currently eight full-time professionals, plus two open slots and another two people with a dotted line to Gevertz, is organized and dedicated:

***continued on 10***

the planning and implementation of initiatives that involve personal information. Reactive practices are only involved when needed or called upon, are consulted at specific intervals throughout the activity and are not well integrated into initiatives involving privacy. Maturity of programs and growth of company size play a clear role, shifting the focus of privacy programs from compliance at early stage to risk-based at maturity.

As further detailed below, proactive and reactive programs are not spread evenly across the ecosystem. Rather, certain market conditions and regulatory environments foment strategic privacy programs, whereas others generate more compliance-based roles. In their *Stanford Law Review* article, "Privacy on the Books and on the Ground," Berkeley professors Ken Bamberger and Deirdre Mulligan suggest that a proactive approach can drive additional resources and strategic attention to the privacy program. They warn, "a bureaucratic 'compliance'-oriented approach, by which rules of action are communicated in a centralized top-down fashion and intended to be applied by others with little contextual knowledge, can disempower those within organizations who are charged with carrying out policies, constraining internal pressures for greater resources and attention."[6]

## Tools and Resources

A majority of privacy programs use external counsel and consultants, and a good portion, 38 percent, use privacy technology solutions, such as GRC tools, to help with their compliance and governance efforts. Fully 18 percent have employed consumer services, such as call centers, in the past year. Two thirds of respondents report having

[6] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247 (2011).

***continued from 9***

- The first dotted line is a privacy program manager, currently sitting in the Portfolio Management Office.
- The second dotted line is a manager of HR privacy who sits in the HR organization, supporting what Gevertz and the CSO are working on.
- Four of the direct reports will support regional operations, one each in the United States, Latin America, Asia Pacific and the EU (also responsible for the Middle East and Africa, located outside of Paris, where ADP has European offices). Gevertz hired specifically in the EU, is looking to hire in APAC and tasked two existing lawyers with the U.S. and Latin American responsibilities.

"They need to be in region," Gevertz said, "to support both our business operations in those countries (over 50,000 associates worldwide), and our client-facing operations. They need to be close to their clients."

**The in-region privacy pros work closely on a daily basis with the lawyers in those business units and the security teams.**

He said these are not junior people. "I'm looking for people who can develop relationships with the DPAs directly," he said. "I know many of the DPAs around the world, but that's a bad business model. I can't have it just be me."

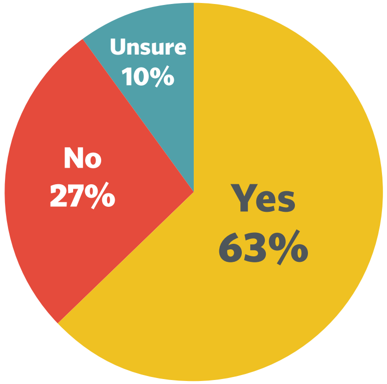
The in-region privacy pros work closely on a daily basis with the lawyers in those business units and the security teams. "It's not dissimilar to what I'm doing," Gevertz said, "but on a regional scale."

***continued on 11***

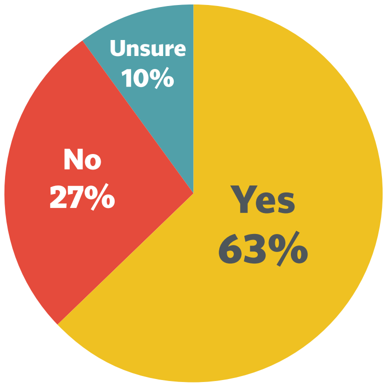
undergone a privacy audit, with firms in regulated industries or privacy operations in the EU tending to run audits internally. A similar proportion of respondents report having a vendor management program related to privacy.

Expect that last number to grow. In recent enforcement actions, the FTC and the Federal Communications Commission (FCC) have made clear that vendor management is a critical component of a privacy and data security program. The FCC, for example, fined AT&T $25

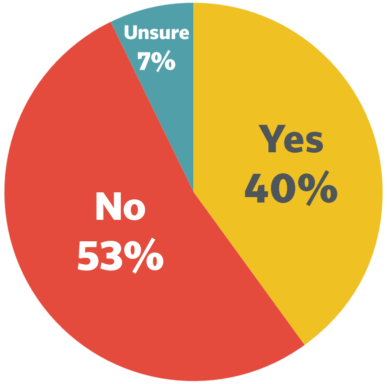
**Have Vendor Management Program**



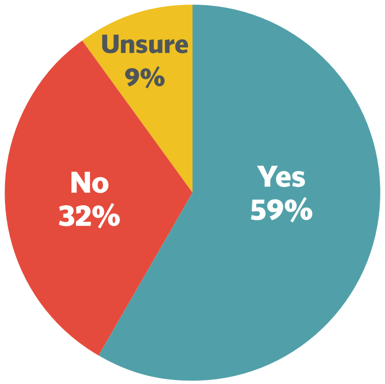
**Use of Internal Audit for Privacy**



**Have Privacy Working Group**



**Use PIAs**



***continued from 10***

The team member tasked with Latin America also works on the global accountability program, focusing on Safe Harbor and the BCRs and helping to build a privacy management accountability framework (they're working with Nymity on this).

There is also a full-time analyst working on these efforts, focusing on the cookie compliance program and other issues.

The privacy pro focusing on the United States also has oversight of all of incident response. Managing 48 laws in the U.S., plus new ones around the world, eats up a number of hours.

That person has a senior director who reports to her, helping to fully build out incident response policy and oversight. He'd like to add a full-time person in the EU as well, considering the pending GDPR's reporting demands and efforts like the Netherlands' recently passed reporting law.

- Another full-time direct report is a lawyer who focuses on health data protection. With a multitude of businesses that focus on issues like COBRA, FSA accounts, open enrollment procedures and other parts of the employee health lifecycle, there is plenty of work for a dedicated lawyer.

"Often," he noted, "it's not technically PHI, but we want to protect it as if it were, so that's what they do."

- The final full-time staffer is a privacy engineer. For example, "we're building our nextgen platform to do what we do, global human capital management,

***continued on 12***

million for a data breach that occurred in contracted call centers in Mexico, Colombia and the Philippines.[7] In *GMR Transcription*, the FTC expanded its third-party liability doctrine, holding a company directly responsible for the consequences of a service provider's security flaws.[8]

Alas, existing vendor management programs receive less than stellar reviews, with only 20 percent describing them as very thorough (62 percent somewhat thorough, 17 percent not very thorough or not thorough at all), and only between 25 percent and 33 percent of respondents reporting an on-site or independent audit requirement for most vendors under the program.

In terms of technological solutions, 40 percent of all privacy pros use governance, risk management and compliance (GRC) tools, with RSA Archer the most often cited and Oracle and SAP GRCs coming in a distant second and third. Data protection controls (privacy and security) are the most common of GRC tools, with other common uses involving vendor management and remediation of gaps identified in audits.[9] In addition, 60 percent of professionals use Privacy Impact Assessments (PIAs), with about half saying PIAs are part of their company's Systems Development Lifecycle process. Over the past decade, PIAs have gone mainstream, with businesses, regulators and industry groups creating tools, guidelines and best practices for PIA deployment.[10]

[7] In the Matter of AT&T Services, Inc., Federal Communications Commission Order, April 8, 2015, http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0408/DA-15-399A1.pdf.

[8] In the Matter of GMR Transcription Services, Inc., et al, Federal Trade Commission, Decision and Order, August 14, 2014, https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf.

[9] *Also see* EY, Building Trust in the Cloud: Creating Confidence in Your Cloud Ecosystem, June 2014, http://www.ey.com/Publication/vwLUAssets/EY_-_Building_trust_in_the_cloud/$FILE/EY-grc-building-trust-in-the-cloud.pdf.

[10] Information Commissioner's Office, Conducting Privacy Impact Assessments: Code of Practice, 2014, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

**continued from 11**

worldwide," Gevertz said. The privacy engineer is sitting with that team and is integral to the platform's development as the team puts it together in Manhattan.

In general, "We're developing in a very agile environment," Gevertz said, "so I can't do privacy periodically. I need to do privacy live. This is a person with tech and coding experience who has done privacy for a long time and sits in the scrums, develops privacy by design training, and that was one of the best things that I've done … I could use three more of them."

This person is also spearheading work exploring new issues that arise as ADP gets into the world of monetizing big data. "Some people say we have a lot of data," Gevertz chuckled. "I say, 'We don't have it. Our clients do.'"

However, most contracts say ADP can use anonymized data for analytical purposes, so his team is charged with working with data scientists and technologists in anonymizing data, aggregating it and using it to create value for ADP clients.

**I can't do privacy periodically. I need to do privacy live.**

- Finally, there is the team's work with other teams. The full-time privacy engineer sits on the IT team's architecture review community. Representatives of all the product development teams sit on that and meet monthly.

The health lawyer sits on the health data protection council, which brings together representatives of more than 20 different parts of the organization. Privacy is the co-executive sponsor of that council, which brings together

**continued on 13**

## How Regulation Affects Operations

The results of this part of the survey may at first seem counterintuitive. The less privacy regulation the more developed the privacy program? Could it be that on average, the most developed privacy programs are found in sectors, such as software and marketing, which in the U.S. are *not* subject to sectorial privacy laws? Even in countries, such as Canada and EU Member States, where an omnibus cross-industry statute governs privacy, industries such as banking and healthcare remain subject to additional layers of regulation. Why do privacy practices in these industries appear less robust than in less regulated sectors?

### Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Staffing** | | | | |
| Mean number of employees dedicated to privacy | 12 | 10 | 10 | 17 |
| Expect full-time dedicated staff to increase | 31% | 23% | 34% | 30% |
| **Budget** | | | | |
| Median budget for privacy | $277,025 | $130,000 | $250,000 | $300,000 |
| Expect budget will increase | 31% | 25% | 32% | 35% |
| Less than sufficient to meet privacy needs | 59% | 70% | 60% | 52% |

## Unregulated Industries

The survey compares the investment in privacy of companies in regulated industries, such as banking and healthcare, to that of companies in unregulated industries, such as marketing and software, and that of government agencies. The data demonstrates that the median budget for privacy in unregulated firms ($300,000) is more than double that of government ($130,000) and 20 percent higher than that of regulated businesses ($250,000). Headcount is commensurate with budget, with unregulated companies reporting an average of 17 employees in the privacy team compared to 10 employees in regulated businesses and government.

Upon closer reflection, however, it becomes clear that the privacy profession, which has risen from the ground up—based not on legislative fiat or regulatory necessity, but rather on a growing perception and understanding among businesses of the strategic value of data and the reputational impact of sound data governance—will thrive in unregulated environments where ethical lines remain undrawn. Privacy underlies consumer trust and expectations. It draws on professionals' ethics and communications skills to identify the fault lines between new technologies and existing social values. Privacy professionals are trained to predict the reaction to a new product, service or app by consumers, regulators, advocates and the press. The answers are seldom written in law. Even

***continued from 12***

a lawyer and an operations leader from each business unit that touches health data.

The dotted line in HR is the staff for the HR privacy council, of which Gevertz is the executive sponsor, along with the head of HR Shared Services. Every country in which ADP operates is represented by someone on that council, which oversees HR privacy issue for the 50,000-plus employees around the world.

where they are, companies should not settle for compliance with the law. Even if it's not illegal, it may still be misguided.[11]

### Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Main Reasons for Privacy Program** | | | | |
| To reduce risk of data breach notification/publicized data breaches | 77% | 70% | 82% | 72% |
| To enhance the company's brand and public trust | 61% | 50% | 61% | 66% |
| To meet consumer expectations and enhance trust | 60% | 49% | 63% | 65% |
| To meet the expectations of business clients and partners | 54% | 33% | 56% | 61% |
| To enable global operations and entry into new markets | 29% | 3% | 25% | 40% |
| To provide a competitive differentiator | 26% | 3% | 26% | 39% |

Accordingly, not only is the investment in privacy greater for unregulated companies, but also the function is more strategic. Unregulated businesses report a greater focus than regulated businesses or government entities on enhancing the company's brand and public trust, meeting consumer expectations and fulfilling the needs of business clients and partners. These numbers are particularly salient for businesses in the software and services sector. Not surprisingly, the privacy programs of unregulated businesses tend to be risk-based (52 percent) rather than compliance-based (37 percent), a mirror image of the results for government programs (49 percent compliance-based; 41 percent risk-based). "Risk," of course, means not only risk to the organization,

[11] J. Trevor Hughes & Omer Tene, *The Truth Is Out There: Compliance and Security Are Not Enough*, Privacy Perspectives, Oct. 3, 2014, https://iapp.org/news/a/the-truth-is-out-there-for-big-data-privacy-compliance-and-security-are-not-enough.

## CASE STUDY: Leveraging Privacy Working Groups To Prioritize Resources

**Chief Privacy Officer Susan Bandi** arrived at Monsanto three years ago to fill a gap. While there were a number of specific privacy policies and procedures, there was no documented formal "privacy program" to speak of, "and, based on our global nature and footprint, we wanted to ensure that we did everything we needed to do to be a leader in this rapidly changing space."

Yes, like 23 percent of all privacy professionals surveyed, Bandi, constructed the program she currently heads, but this isn't her first rodeo. With 13 years experience in security and privacy with Enterprise Holdings, Bandi who is not an attorney, is perhaps ahead of most three-year-old privacy programs in that she has plenty of lessons learned to build on and implement to ensure the program continues to mature; it has quickly moved from an "early stage" program, like 19 percent of respondents, to a documented, repeatable and integrated program.

First, she had leadership buy in. Monsanto's CIO recognized the need for a formal program headed by a privacy veteran and brought Bandi in, immediately making her the chair of a privacy steering committee that includes the Chief General Counsel, the VP/Controller, the CIO and the CISO, to whom Bandi now reports directly (just 14 percent of respondents are located in information security).

"For me, privacy has always been part of the IT Security organization, so it seems normal" to report to the CISO, she said. "As part of IT Security I can influence specific decisions and ensure alignment between compliance and security."

***continued on 15***

for example, through legal liability, but also to individuals whose privacy may be affected.[12] This is captured in risk-based programs' focus on strengthening brand, trust and consumer expectations.

Unregulated businesses are more focused on enabling global operations and entry into new markets, and, importantly, positioning privacy as a competitive differentiator.[13] More than equivalent figures in the general market, privacy professionals in unregulated industries also reported a much higher instance of interacting with their corporate marketing departments and product teams, the hallmark of privacy by design. In regulated industries, in contrast, privacy professionals engage most with regulatory compliance and internal audit. Moreover, privacy professionals in software and services firms report a far greater influence over product managers (75 percent), product engineers (73 percent) and product designers (72 percent) than general industry numbers (56 percent, 51 percent and 53 percent, respectively).

An approach to privacy governance that transcends regulatory compliance has academic pedigree. Bamberger and Mulligan observed that while the dominant narrative regarding the regulation of privacy in the United States and the European Union, which depicted the U.S. approach as a loose patchwork compared to the European omnibus FIPPs-based model, correctly described privacy *on the books*, it failed to accurately describe the profound transformation of privacy governance practices *on the ground*.

[12] Martin Abrams, The Essential Elements of Accountability, Information Accountability Foundation, 2013, http://tiaf01.ipower.com/wp-content/uploads/2013/09/The-Essential-Elements-of-Accountability.pdf.

[13] Heidi Shey, *Privacy Becomes a Competitive Differentiator in 2015*, Forrester Blog, Nov. 12, 2014, http://blogs.forrester.com/heidi_shey/14-11-12-privacy_becomes_a_competitive_differentiator_in_2015.

***continued from 14***

She says, because of this, she absolutely has the visibility and support she needs to put her vision into place. After meeting monthly as the program was launching, the steering committee now meets quarterly, "but I'm at liberty to call an emergency meeting if I feel we need to get together."

This steering committee is "very risk-and compliance-focused," Bandi said. From this group, she gets direction on what the appetite for risk is on a certain project or as part of a certain initiative and she can use that to guide her proactive priorities for the privacy team.

**You need to stay in alignment with what the company strategy is.**

However, that's not the only privacy working group in the organization (only 40 percent of privacy pros surveyed have a privacy working group at all in their organization). There is also a core operational privacy working group that includes several Monsanto attorneys (including one dedicated primarily to privacy and another to ethics and business conduct), a privacy professional dedicated to EMEA and a compliance leader for Human Resources. Agenda items always include compliance work, upcoming legal requirements and "watch" items for the organization—those pending regulations or laws that may impact the company down the road.

The EMEA representative is vital, Bandi said, "because so many emerging laws model after the EU directive." There is a second full-time privacy compliance employee in EMEA, as well as a data protection officer in Canada, who is supported by staff in the main U.S. office. About 30

***continued on 16***

### Privacy Professionals Work with

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Interact with on a regular basis …** | | | | |
| Regulatory Compliance | 64% | 48% | 73% | 60% |
| Internal Audit | 45% | 30% | 49% | 45% |
| Marketing | 42% | 10% | 42% | 51% |
| Product Managers | 40% | 12% | 39% | 56% |
| Records Management | 39% | 66% | 41% | 24% |

Bamberger and Mulligan noted that, more than their European counterparts, American corporations committed significant resources to privacy, including by employing chief privacy officers and other privacy professionals, undertaking privacy certification and training and developing privacy seal and certification programs. To help guide these developments, major law and consulting firms established new and growing privacy practices. Bamberger and Mulligan characterize this approach as comprising "a high level of attention, resources, and prominence for the privacy function within the firm; the integration of privacy decision-making into technology design and business-line processes through the distribution of privacy expertise within business units and assignment of specialized privacy staff to data-intensive processes and systems; and a high-status privacy lead who mediates between external privacy demands and internal corporate privacy practices."[14]

It has become clear that managing privacy is not simply a compliance role. It entails channeling the moral voice of the organization. With companies becoming laboratories

[14] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, 81 Geo. Wash. L. Rev. 1529, 1638 (2013).

***continued from 15***

percent of respondents said their programs are similarly geographically distributed.

Further, sub working groups are pulled together for certain projects, Bandi noted, or certain watch areas "to ensure that we don't miss any gaps."

Perhaps the most important part of her work with the steering committee and working groups is that it gives her insight into the strategies and goals of the organization as a whole. This, she said, is an often-overlooked, but vital, part of a great privacy program.

These efforts, plus her regular meetings with the CIO, "are a very good way to make sure what we want to be doing on the privacy team is in alignment with what we're doing around the world and factor that in," Bandi said. "He's very transparent not just with me, but with others on the strategy of the organization."

Why is that important? "You need to stay in alignment with what the company strategy is," Bandi said, "so that the group responsible for privacy compliance understands what the priorities are three years out, five years out." For instance, she said, it can help to know that there's a strategy for growth into a specific region of the world, so you can undertake due diligence and provide information that becomes part of the decision-making as they prioritize expansion.

"You want to be in front of that," said Bandi. It can cause friction and inefficiency if the priorities of the privacy team aren't aligned with the priorities of the company as a whole. "I think that's one thing that maybe people miss," she said, "especially someone new to the space." ⬢

for big data research, data ethics have become a critical component of corporate governance frameworks. Companies can no longer simply view privacy as a compliance matter to be addressed by legal departments or a technical issue handled by IT. Rather, to avert public embarrassment and consumer backlash, they must consider ethical review processes and instill issue-spotting skills in employees throughout the organization. Indeed, Jules Polonetsky, Omer Tene and Joseph Jerome suggested industry adopt internal review board-like structures (IRBs) to vet the ethical dimensions of innovative data projects.[15]

## Regulated Industries

Predictably, respondents from regulated industries report a focus on accountability processes, the hallmark of compliance-focused programs, including internal audits, vendor management, and the creation of a privacy working group. Government programs, while using privacy impact assessments (PIA) more than their private sector counterparts, use vendor management only half as often (35 percent compared to 69 percent in regulated industries and 66 percent in unregulated). According to certain press reports, such a program could have helped the government contain the risks that materialized in the data breach at the Office of Personnel Management.[16]

At the same time, the structured nature of privacy

[15] Jules Polonetsky, Omer Tene and Joseph Jerome, *Beyond the Common Rule: Ethical Structures for Data Research in Non-Academic Settings*, 13 Colo. Tech. L. J. 333 (2015).

[16] Sean Gallagher, *Encryption "Would Not Have Helped" at OPM, Says DHS Official*, ArsTechnica, Jun. 16, 2015, http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/ ("A consultant who did some work with a company contracted by OPM to manage personnel records for a number of agencies told Ars that he found the Unix systems administrator for the project 'was in Argentina and his co-worker was physically located in the [People's Republic of China]. Both had direct access to every row of data in every database: they were root…'").

## CASE STUDY: Rise of the Data Privacy Coordinator

What privacy risks could there be at Caterpillar, a firm selling heavy equipment largely through an independent dealer network with some direct sale businesses, and how does Caterpillar manage that risk?

That's a good question for **Mark Oram, Corporate Counsel at Caterpillar**, who is also responsible for managing the global data privacy program at Caterpillar. At Caterpillar, data privacy is one of the compliance areas and risks managed through the Ethics & Compliance Program, which is overseen by the Chief Ethics and Compliance Officer.

Oram works in the Legal Services Division of Caterpillar and reports through the Chief Ethics and Compliance Officer, like 16 percent of privacy leads globally, who reports to Caterpillar's General Counsel.

Working with Mark to manage the data privacy program are three other regional lawyers who are regional data privacy risk owners. These attorneys each report up through their own regionally managed groups within Caterpillar's Legal Services Division and, while not through Oram, ultimately to Caterpillar's General Counsel. This is relatively rare, with just 27 percent of privacy pros saying their privacy "team" reports to a number of different positions. Further, just 23 percent of privacy professionals are regionally distributed.  But as Oram pointed out, "it has been helpful to have the regional risk owners be lawyers who are embedded in the region supporting

***continued on 18***

**Larger firms have a strategic focus and more privacy resources**

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Compliance- versus risk-based** | | | | |
| Compliance-based | 41% | 48% | 43% | 35% |
| Risk-based | 47% | 42% | 45% | 53% |
| **Staffing** | | | | |
| Mean number of employees dedicated to privacy | 12 | 2 | 5 | 24 |
| Expect full-time dedicated staff to increase | 31% | 17% | 31% | 41% |
| **Budget** | | | | |
| Median budget for privacy | $277,025 | $75,000 | $250,000 | $1,000,000 |
| Less than sufficient to meet privacy needs | 59% | 57% | 65% | 55% |
| Proportion of privacy budget allocated to salary and travel | 51% | 45% | 51% | 54% |
| Proportion of privacy budget allocated to professional development | 9% | 12% | 8% | 8% |

programs in regulated industries allows professionals to report higher than average career opportunities in privacy in their organization. For example, in the banking industry, 59 percent of respondents see a moderate/strong career path in privacy compared with a 46 percent cross-industry average. The career prospects for privacy are starkly different in government, where 58 percent of respondents report no/low career opportunity in the privacy group, compared to a cross industry average of 46 percent.

## Organizational Size and Maturing Operations

The results in this part of the survey do more than merely state the obvious—that large companies invest greater resources in privacy and that mature programs have more resources and employees than those in early and mid-stage. Rather, they chart a path for growth for small enterprises and early stage programs, who can gain insight into where they stand and how they can expect to evolve within one, two or five years. More importantly, they help businesses benchmark their privacy programs against

***continued from 17***

the business—not only are they familiar with other, non-privacy laws relevant in the area, but they are also familiar with Caterpillar's business and processes and practices in that region."

In addition to Oram and the regional risk owners, there is a network of privacy individuals throughout Caterpillar, both in Legal Services Division and embedded in the business who drive the data privacy program. For example, there are in-country lawyers with data privacy expertise and other individuals in the business who deal with privacy issues more frequently. As Oram explains, "Caterpillar is a complex matrix organization with business units and companies spanning the world, and it is not uncommon to have a team with diverse responsibilities working together and for people to have multiple dotted line reporting structures."

This is not particularly rare, as just 44 percent of in-house privacy pros report that privacy is their full-time consideration.

Full-time privacy professionals at Caterpillar? As the owner of the data privacy program, Oram and a dedicated paralegal are formally the only two individual whose job roles are specifically dedicated to data privacy, but there is a network of professionals working with them. Additionally, fairly recently there was a new role created at Caterpillar to standardize processes and create an accountability agent for data privacy. These are Data Privacy Coordinators and each Caterpillar legal entity with employees has one. There are approximately 50 Data Privacy

***continued on 19***

similarly situated competitors. How much are competitors spending? Where do they house privacy in their corporate governance scheme? What are the assignments and responsibilities of their privacy professionals? Which projects should they accomplish over the next year or two (*e.g.*, data inventorying and mapping, policy revisions, privacy audits and assessments, vendor and third-party assurance, data loss prevention technology, training and certification). After all, regulators in this space, particularly the FTC, have repeatedly alluded to industry best practices when evaluating businesses for privacy and data security compliance.[17]

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Internal and External Resources** | | | | |
| Have worked with privacy attorney in past year | 66% | 56% | 65% | 74% |
| Uses internal audit for privacy audits | 63% | 54% | 58% | 73% |
| Have a Privacy Working Group | 40% | 33% | 38% | 46% |
| Have Vendor Management Program | 63% | 48% | 66% | 71% |
| Use GRC tools | 42% | 18% | 42% | 58% |
| Have centralized Contract Management System | 35% | 34% | 40% | 31% |
| Use Privacy Impact Assessments (PIAs) | 59% | 52% | 58% | 64% |
| **Involved in creating privacy program** | 57% | 70% | 62% | 45% |

As expected, there is a close correlation between the maturity of privacy programs and the size of respondents' corporations. Forty-eight percent of large companies also have mature privacy programs; and 88 percent have middle to mature programs. In comparison, only 25 percent

[17] Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 San Diego L. Rev. 809 (2011).

***continued from 18***

Coordinators supporting Caterpillar's approximately 160 legal entities that have employees. Most of the Data Privacy Coordinators reside in the HR department.

As Caterpillar looked at who should act as accountability agents for the personal data the company held, "the logic we went through," said Oram, "is that we realized we needed to have centralized figures who we could go to, and we wanted to select roles that would provide for the most consistency and be efficiently placed." A number of projects requiring reoccurring global coordination involved HR data. "There is a certain appeal to having the accountability agents being in HR," Oram said, "the argument was, where we have employees in a legal entity, we know that that company has privacy issues—both because we have information about those employees and because those employees may be processing personal information of others." Given the desire to have the program, including the accountability agents, as consistent as possible across the enterprise and HR's receptiveness to make implementations and roll-outs more efficient, HR agreed to host the role of Data Privacy Coordinator.

**There is a certain appeal to having the accountability agents being in HR.**

In fact, said Oram, one part of the process inside Caterpillar isn't too different from a firm registering with a DPA as a data controller. If an employee is collecting

***continued on 20***

of small companies have mature programs. On average, programs identifying as mature were established 11 years ago, compared to only two years for programs reporting as early stage.

The survey results reveal a clear progression from an initial focus of privacy programs on compliance to a risk-based approach. Large companies with mature privacy teams characterize their programs as risk-based, whereas small companies and early-stage programs report an emphasis on compliance. This is not surprising, as companies first devote resources to complying with the law, and later expand the scope to address extra-legal, more strategic concerns about brand, reputation, trust, consumer expectations and global expansion. Interestingly, compared to smaller entities, large companies also place a premium on using privacy to enhance not only consumer, but also employee, trust.

Predictably, large companies have larger privacy teams in terms of both staffing (average staff of 24 compared to two for small companies) and budget (median budget of $1 million compared to just $75,000). In addition, in large companies, fewer privacy professionals report being engaged in non-privacy activities. Hence, with size and maturity comes the recognition that privacy is not something done off the side of an HR or finance manager's desk, as well as the ability to devote sufficient resources to address the issue. Accordingly, large and mature programs are more likely to have a program leader who is entirely dedicated to privacy. Here, stark differences emerge between large and smaller companies. Fifty-one percent of large companies report a privacy leader devoted full-time to privacy tasks compared with only 13 percent of small companies.

The maturity of a privacy program is manifest in the range of resources and tools it deploys. This typically includes

***continued from 19***

personal data with an intention to use it in some way, that employee needs to inform the Data Privacy Coordinator applicable to their business about what personal information they are collecting, the purpose of processing, etc. But this is still a relatively new process. "It's an area where we're doing a lot of work," he said. "In a number of situations, we already needed to have the metadata about personal information—for example to complete government registrations. Expanding this allows for having consistent processes that allows for better understanding the data flows—after all, privacy is about the personal information. Additionally, we're working on additional tools, such as a privacy impact assessment to identify gaps and how to close them."

A lot of changes are potentially in the offing for Caterpillar as its privacy program matures. "This has been a fairly aggressive year in taking the program and maturing it," Oram noted. "We've had an enterprise policy since about 2004 that established core principles that were in a large part based on the Safe Harbor. And as we looked at [binding corporate rules] earlier this year, codifying the network of Data Privacy Coordinators and other requirements, we saw an opportunity to update the enterprise policy and supplement it with a more detailed enterprise procedure."

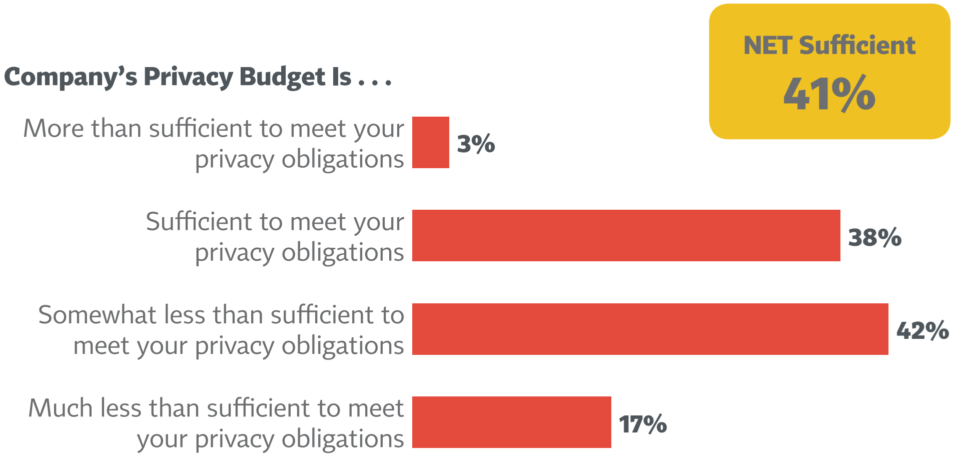
So, last year Caterpillar revised its enterprise policy and put in place a new privacy enterprise procedure. The policy is still "principle" based; however, the procedure includes defining the governance, roles (e.g., Data Privacy Coordinators) and other requirements.

***continued on 21***

working with external privacy consultants, undergoing privacy audits, employing vendor management programs, using GRC tools and performing privacy impact assessments (PIAs). Forty-six percent of large companies and 43 percent of mature programs have privacy working groups, helping their chief privacy officers perform their tasks. Large companies and mature programs also branch out to interact with other departments on a regular basis, including information security and IT, legal and compliance, HR, internal audit and marketing. Firms with mature programs also report engagement with product managers.

Recognizing existing gaps, early- and mid-stage programs state they would like to have more influence over nearly every function in the organization. Perhaps reflecting a response to what some privacy professionals view as a cavalier approach to data innovation on the part of start-up companies, an overwhelming majority of respondents in the smallest firms state they would like to have more influence specifically over corporate ethics.

## More than half of privacy pros feel budget is insufficient



*continued from 20*

The updated policy and new procedure launched on Data Privacy Day in January of 2015 along with a data privacy handbook that provides background, explanations and forms and templates for meeting the requirements of the enterprise policy and procedure.

**Last year Caterpillar revised its enterprise policy and put in place a new privacy enterprise procedure.**

This solidified the Data Privacy Coordinator network, entrenching in enterprise procedure a requirement to notify them of any new personal data collection or processing.

In this way, Caterpillar is able to manage the risk from both directions: both from the top of the executive ladder and on the ground floor. "It's an interesting dynamic," said Oram, getting at the very definition of owning the risk. Ultimately, the data owner has accountability, as they're collecting the data and are best situated for making decisions about how it's handled. "But they have to meet the requirements of the enterprise—both from a compliance perspective and a risk perspective," he said, "We are setting clarity around that. It's about building a program to

*continued on 22*

Sophisticated data professionals recognize that privacy is not a management function that can remain detached from operations, product engineers and marketing teams. Indeed, integrating privacy into product design and manufacturing teams is the hallmark of privacy by design. Accordingly, only 19 percent of large companies report that privacy teams are located exclusively at corporate headquarters compared to 78 percent reporting teams that spread out between corporate headquarters and regional offices. The figures for mature programs are similar, with decentralized structures controlling.

Importantly, mature stage programs report a higher likelihood of involvement from the outset in data-related projects (39 percent compared to 23 percent in early-stage programs), and involvement in projects on an ongoing basis (56 percent compared to 31 percent in early-stage programs). In contrast, early-stage programs are more likely to be brought in only when needed (41 percent compared to 17 percent in mature programs.) Privacy by design starts at the earliest stage of product development. Inexorably, organizations are coming around to that conclusion as they climb the maturity curve.

## Large ≠ Mature

Although large companies and mature privacy programs are generally aligned, certain differences remain. That is, mature privacy programs in small or medium companies have some distinct features that less mature privacy programs in large companies do not. For example, unlike simply large firms, companies with mature privacy programs are more likely to have centralized privacy reporting structures.

In mature programs, respondents tend to believe that privacy is housed in the right place in the organization, compared to privacy professionals operating in large firms, who are less likely than their counterparts in small or medium companies to think it is located in the right place. Large firms, more than mature privacy programs, expect budgets and full-time staff to increase. As you might expect, when placed on a maturity curve, it is the less mature programs that expect to grow in terms of staffing and budgets. At the same time, even the largest companies complain that current budgets do not suffice to meet privacy needs.

*continued from 21*

make sure we have the right checks and balances and procedures and that data owners are going through the process where they're answering the right questions and documenting data collection and use.

"So, we're facilitating compliance while getting line of sight to the risk," Oram said, "by emphasizing policies and procedures with standardized requirements."

That line of sight is important at a sprawling organization like Caterpillar to make sure data is being properly handled. Awareness is key, so that each of the many business units is clear on procedure and how to follow it. That means training, assessments and audits to validate that the procedure is working.

As Caterpillar approaches the BCR process, any gaps are being identified and addressed as part of the overall accountability program. Accountability happens in many different ways, and, for Caterpillar, it will be those Data Privacy Coordinators who will be an important building block in the program. ⬢

No one's budget, it would seem, is sufficient for the challenges privacy presents.

## Region

While not capturing the totality of the European data protection market, the survey provides good insight into the practices of global, mostly American-based businesses operating in Europe. Some interesting comparisons can be drawn between privacy programs in these entities and those across the pond in the U.S.

For starters, a greater proportion of European respondents reported their program leader focused exclusively on privacy than in the U.S. European programs tend to cluster around the mid-maturity stage, with fewer respondents reporting early-stage programs on the one hand or mature programs on the other hand than their U.S. counterparts. American-based programs are significantly larger in terms of both budgets and staffing, with median budgets for privacy in the U.S. more than double those in the EU. At the same time, a greater proportion of American respondents expect privacy budgets to grow than those in Europe.

The main reasons cited for having a privacy program are similar across the board, except that Americans are more likely to mention an interest in being "good corporate citizens" as well as a desire to increase the value and quality of data. Interestingly, increasing consumer trust is a higher priority for American companies operating in Europe than for similar companies in the U.S. Given the fallout of the Snowden revelations, American companies may perceive themselves at a competitive disadvantage *vis-à-vis* their EU peers in earning European consumers' trust.[18]

In terms of privacy resources, EU respondents more commonly use internal audit and PIAs, while their American counterparts refer to vendor management platforms and GRC tools. EU respondents are also more likely than those in the U.S. to have met and completed a range of initiatives; the one exception being a greater focus on data loss prevention in the U.S.

Reflecting a more compliance-oriented focus, privacy professionals in the EU would like to have more say in the workings of a whole range of departments, including information security and IT, corporate ethics, HR, and product managers, designers and engineers.[19]

## Conclusion

As the privacy profession establishes itself, important lessons can be drawn from the differences between privacy programs in terms of size, industry regulation and geographic locations. This study has demonstrated that privacy is a growing industry in resources, influence and voice. Privacy programs typically start small, focusing on compliance, before transitioning to larger teams operating a risk-based approach. As programs mature, we see privacy professionals increasingly working more closely with product teams, the security team and large portions of the organization as a whole.

The portrait that this survey paints is that while regulatory compliance remains paramount for privacy programs, organizations are increasingly using tools to mitigate risks, enhance consumer expectations and go beyond the mandates of laws and regulations, with brand and reputation management always in mind. A mature privacy program commonly has more than 20 employees, a privacy

[18] Daniel Castro, *How Much Will PRISM Cost the U.S. Cloud Computing Industry*, Information Technology and Innovation Foundation, August 2013, http://www2.itif.org/2013-cloud-computingcosts.pdf.

[19] Bamberger & Mulligan, *supra* note 12.

leader whose responsibilities focus 100 percent on privacy, a centralized reporting structure with team members disbursed throughout the organization and a variety of resources and tools, including internal audits, vendor management programs, contract management systems and PIAs. Privacy programs deal with compliance and risk management, process documentation and improvement, policy revisions and training and awareness to disseminate privacy throughout the organization.

While it may seem intuitive that new privacy law, like the General Data Protection Regulation, will spur yet more integration of the privacy team into the organization as a whole, our findings run to the contrary. We shall see in further iterations of this survey whether mandated privacy by default and by design actually leads to greater numbers of more mature privacy programs.

iapp

EY

Building a better working world

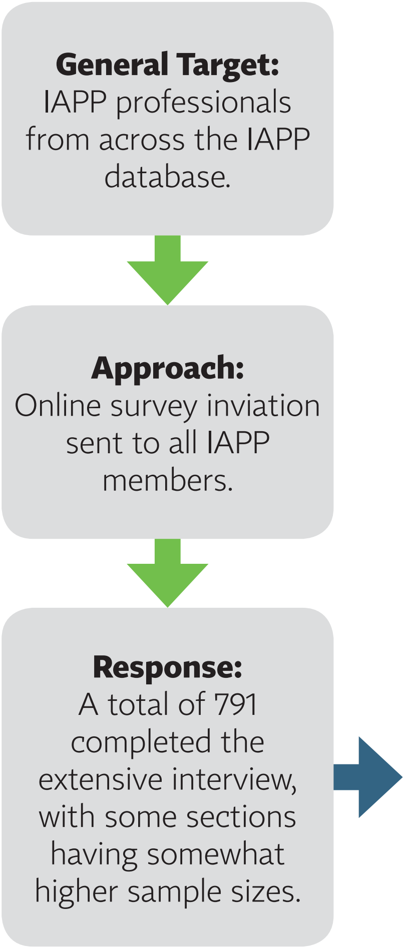
# 2 Demographics

- **Demographics: Background and Method**
- Demographics: Background on All Individuals Surveyed
- Demographics: In-House Privacy Professionals

# Research Objectives

The overarching goal of this research was to provide a profile of how privacy departments and programs are structured within organizations of various sizes and sectors.

# Method



**General Target:** IAPP professionals from across the IAPP database.

**Approach:** Online survey inviation sent to all IAPP members.

**Response:** A total of 791 completed the extensive interview, with some sections having somewhat higher sample sizes.

The survey averaged 23 minutes in length and asked for a variety of detailed information on privacy budgets, employees, salaries and department structures.

**NOTE:** The bulk of this report focuses on responses from **in-house** privacy professionals (from page 34 on).

# 2 Demographics

- Demographics: Background and Method
- **Demographics: Background on All Individuals Surveyed**
- Demographics: In-House Privacy Professionals

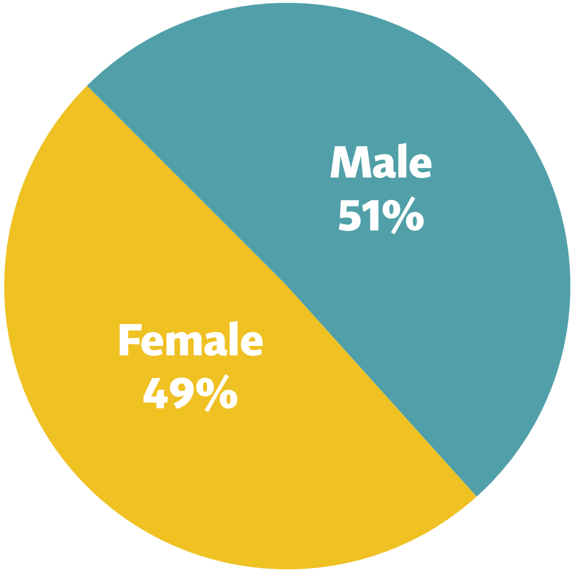
# Privacy professionals are equally split gender-wise, with a mean age of 44

- In addition, 6 in 10 privacy pros have a salary of $100K or more

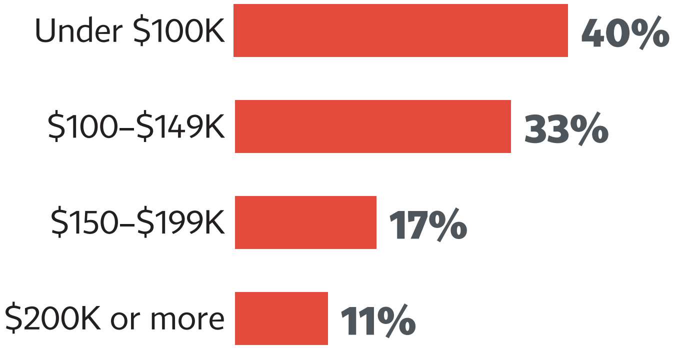
## Demographics of Privacy Professionals

**Mean Age**

**44.0**



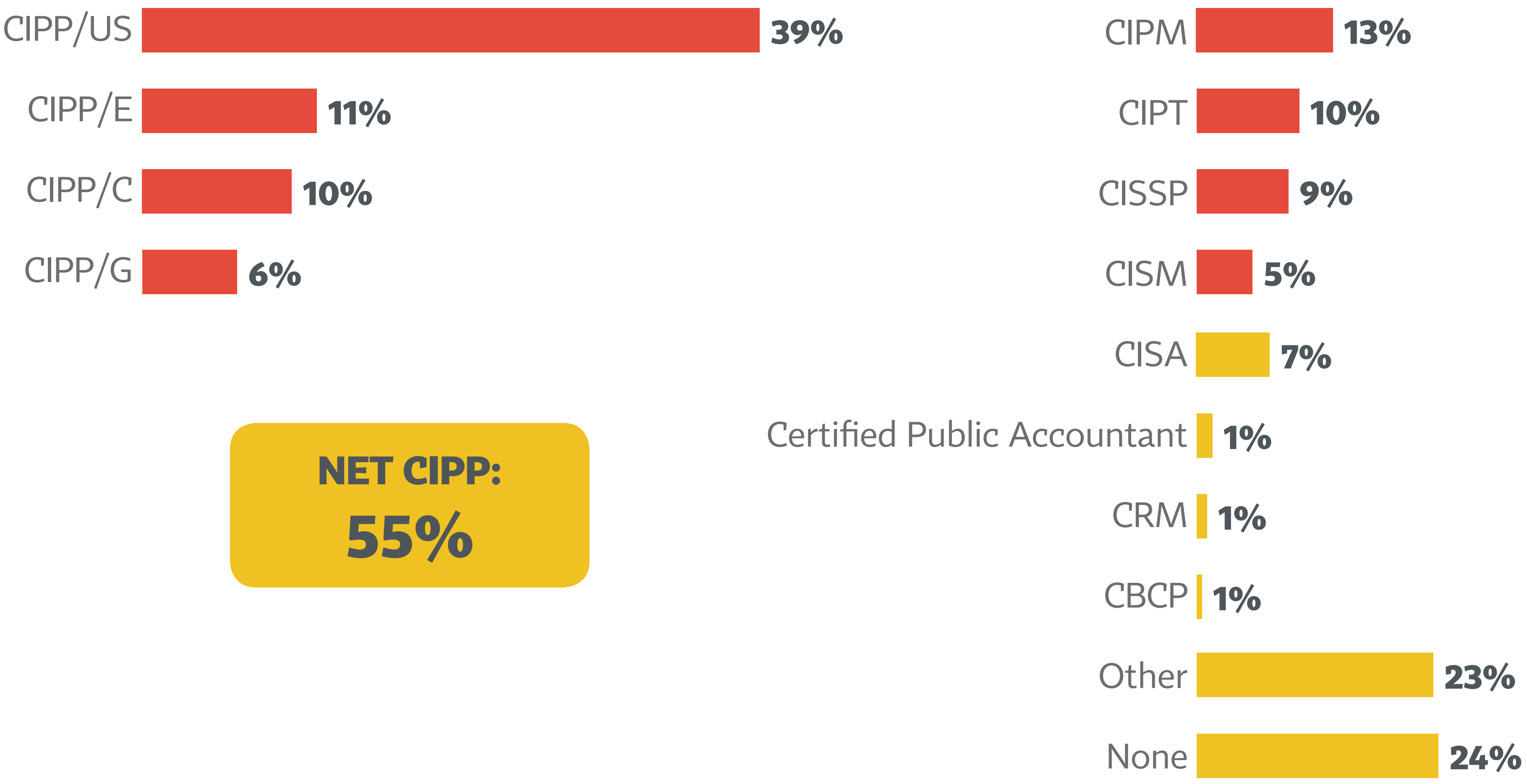
**Annual Income in US$**



I3: What is your age?
I2: Are you…?
B1: What is your current base salary (expressed in U.S. dollars)?

# Three-fourths of privacy professionals have some certification, with most having a CIPP

## Credentials and Degrees Held by Privacy Professionals

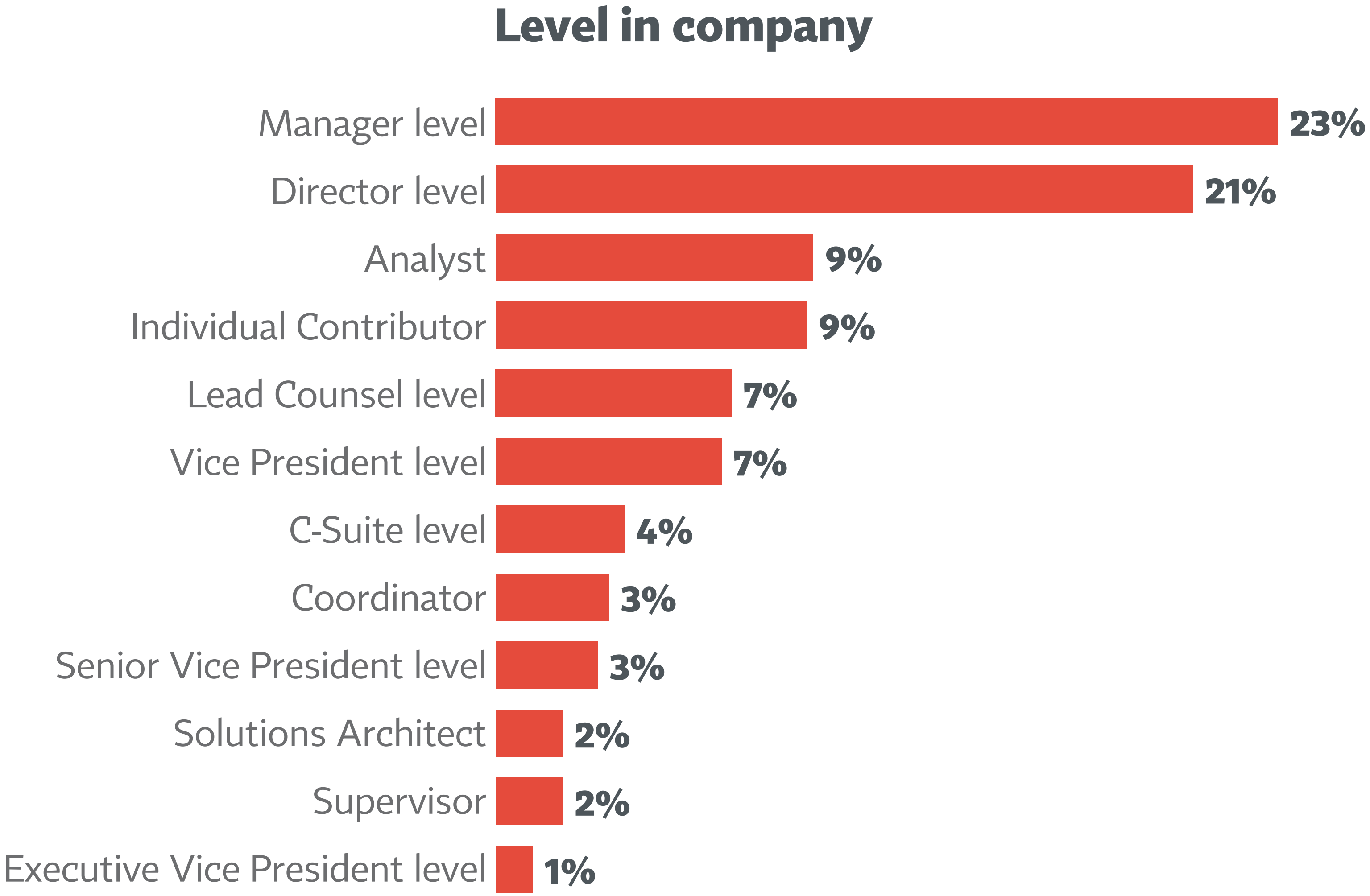


"Other" certifications mentioned include: CCEP, CHP, PMP, ISEB, HIPPAA, CRISC, CRCM, CIAPP, CIA, CHC, CFE, CHP, CAPP

I10: Which certifications do you hold?

# For levels in their organization, the lion's share are managers or directors

- 15% are at the VP level or higher at their firms

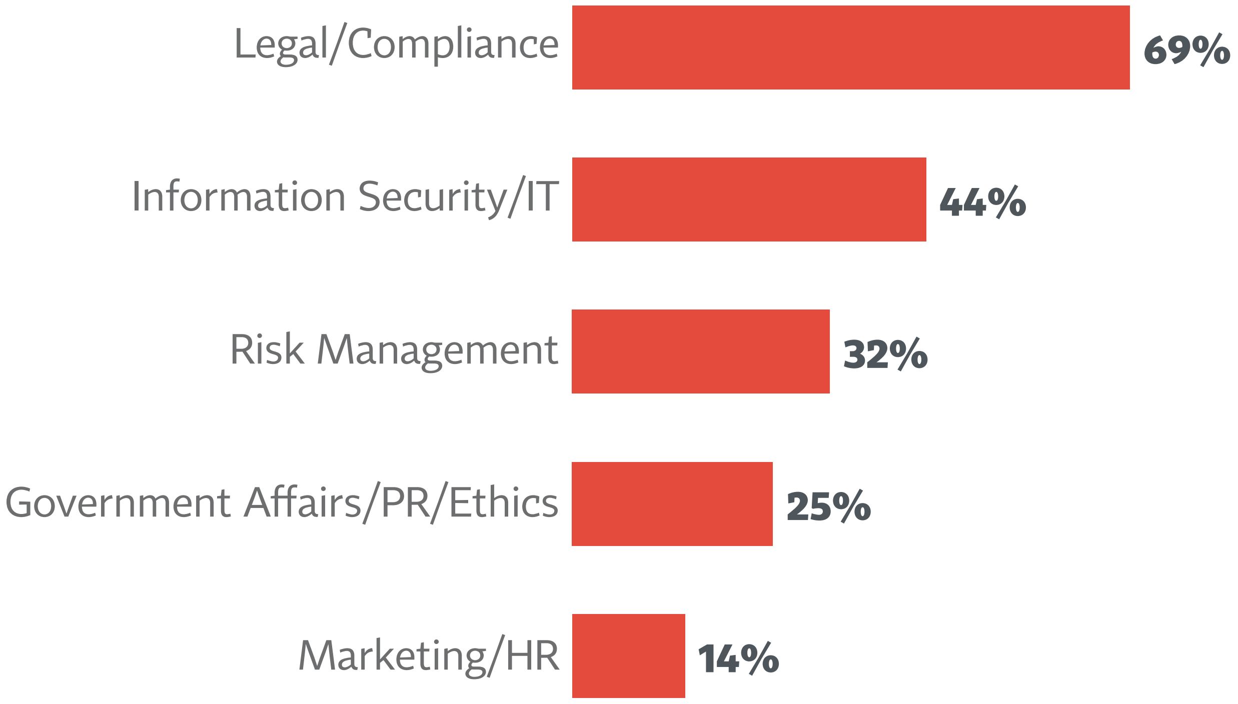


C1: Which of the following levels best describes your position in your company?

# When professionals are asked for the functional areas they work in, they didn't limit themselves to just one

- They work across a range of disciplines, the most popular being legal/compliance and information security/technology.

## Main Functional Areas Work In



C3: Which of the following functions best describe the areas you regularly work in at your company?

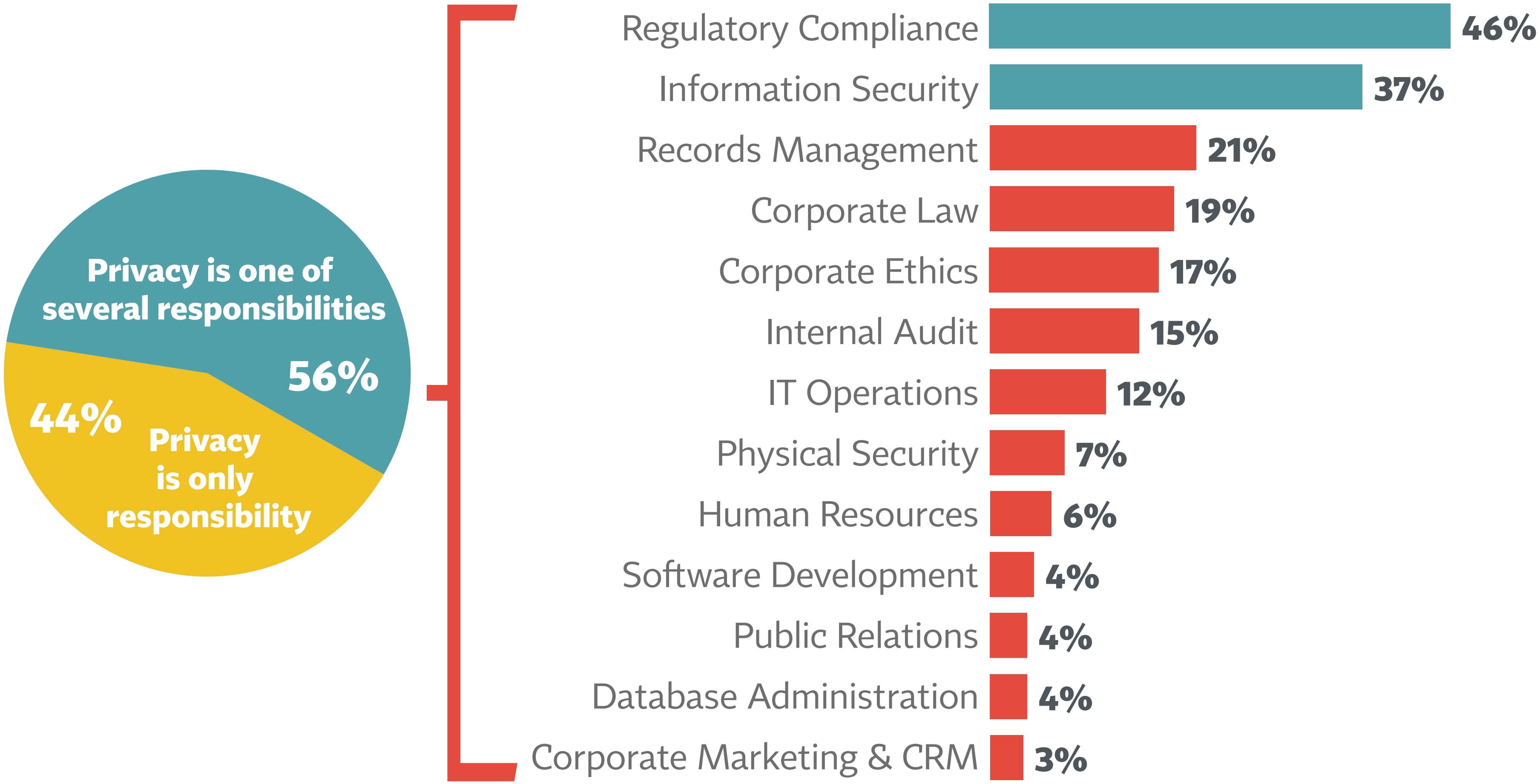
# 2 Demographics

- Demographics: Background and Method
- Demographics: Background on All Individuals Surveyed
- **Demographics: In-House Privacy Professionals**

# Turning to in-house privacy professionals, just 44% consider privacy to be their sole responsibility

- Those who say they have responsibilities outside of privacy are most likely to name compliance or information security as their other areas of focus

## Privacy Responsibility As % of Job

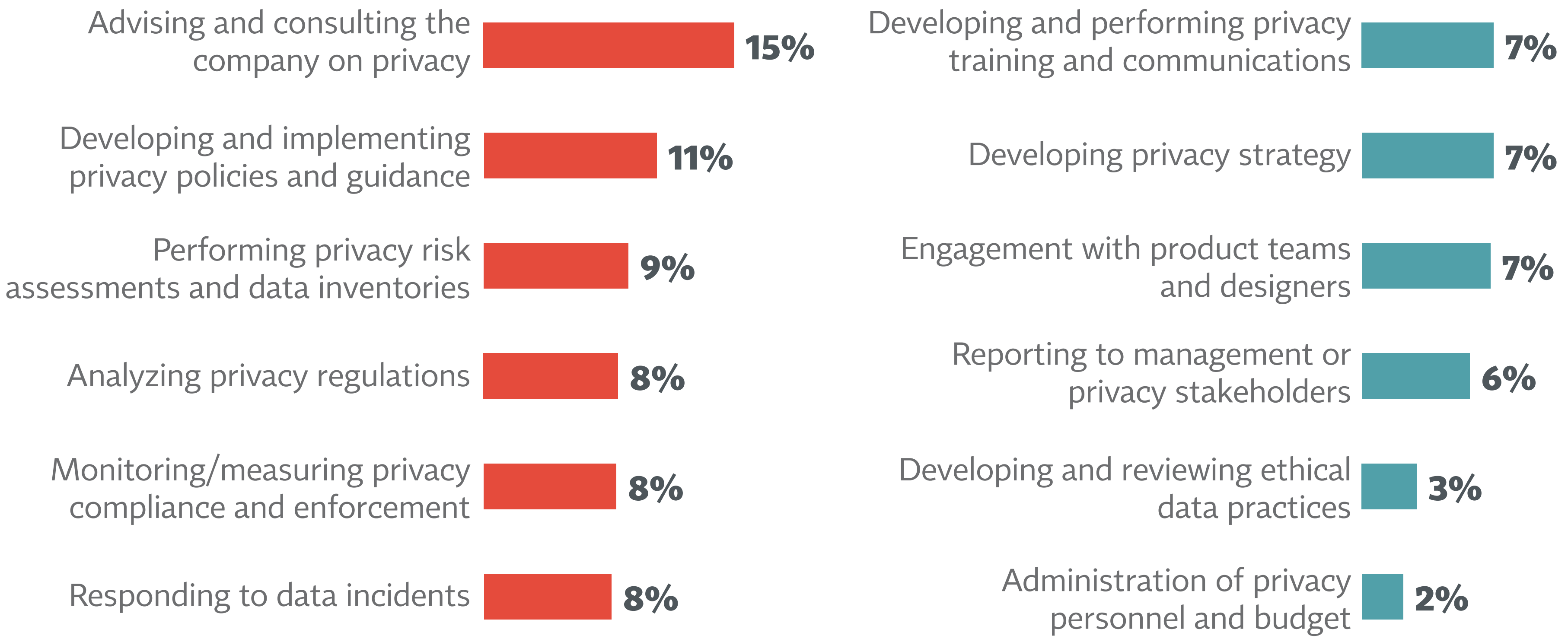


D1: Would you say that privacy responsibilities make up 100% of your work at your corporation, or less than 100%?
D2: In addition to privacy-related responsibilities, what other job functions do you perform in your company?

# Specific privacy tasks are very widely distributed across a broad range of areas

- When privacy professionals are asked to divide their time across different privacy-related tasks, no one task accounts for more than 15%

## Mean Percent of Privacy Work Per Area

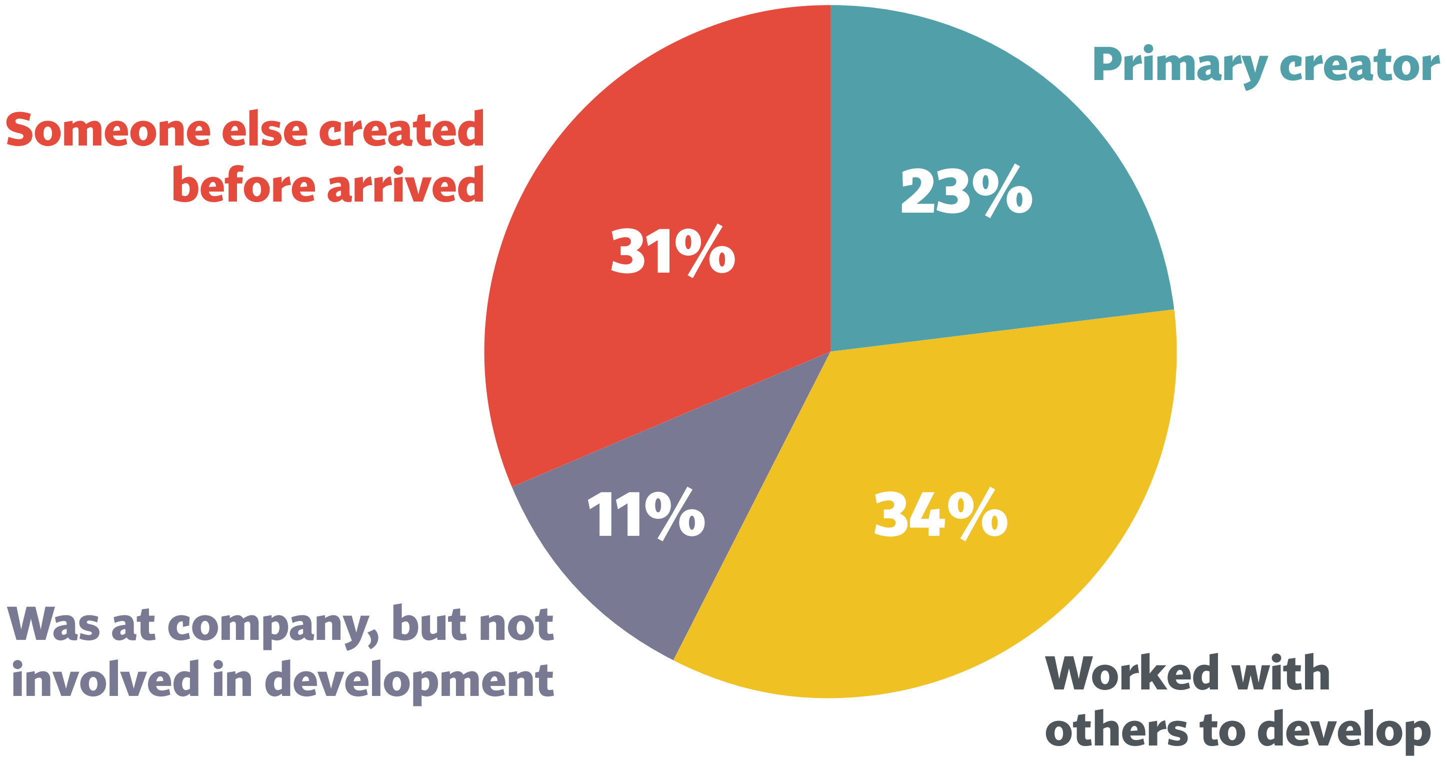


D4: Please estimate the percentage of your privacy work hours that you spend on the following activities.

# About half of the professionals interviewed were directly involved in the development of their privacy program

- And close to one-fourth say they themselves were primarily responsible for creating the program

## Respondent’s Role in Developing Program



E3: Which of the following comes closest to describing your role in developing the privacy program of your company?

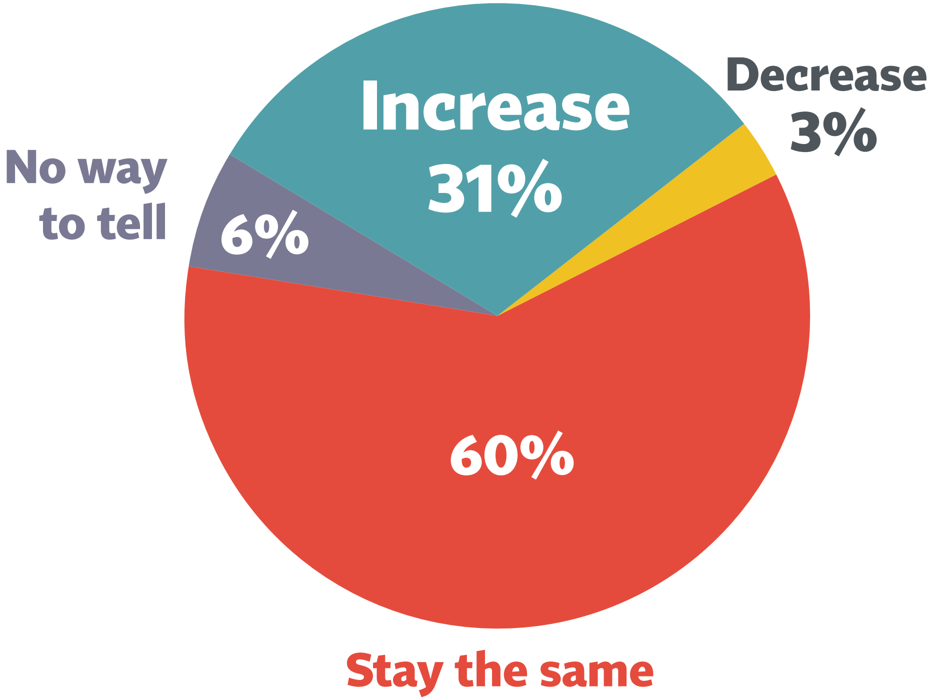
# 3 Privacy Group Characteristics

- **Privacy Group Characteristics: Structure**
- Privacy Group Characteristics: Responsibilities
- Privacy Group Characteristics: Privacy Function in the Business Context
- Privacy Group Characteristics: Internal and External Resources

# Employees dedicated to privacy range from 2 to 24, depending on the size of the company

- Most feel this number will stay the same, but overall, an average increase of 12% is expected.

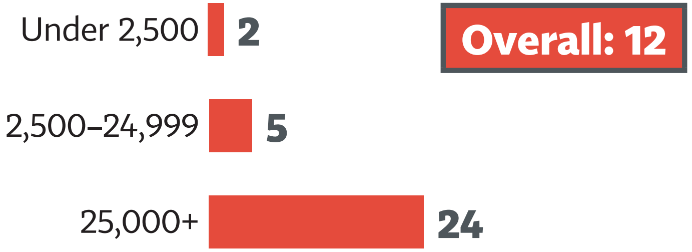
### In Coming Year, Number of Employees Dedicated to Privacy is Expected To:



Expected increase in employees dedicated to privacy:

**+12%**

### Mean Employees Dedicated to Privacy by Size of Company



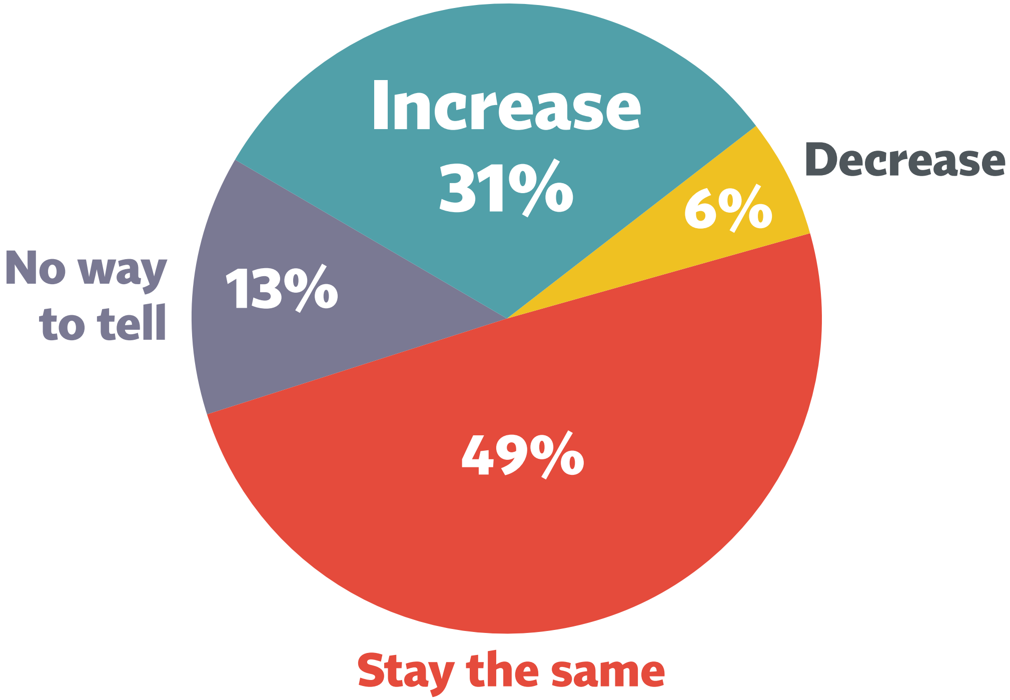
Outliers over 1,000 removed

F1: How many employees are dedicated full-time to your company's privacy program?
F2: In the coming year, do you expect the number of employees dedicated full-time to your privacy program to …
F3: By about what percent do you expect the number of full-time privacy employees to [increase/decrease] in the coming year?

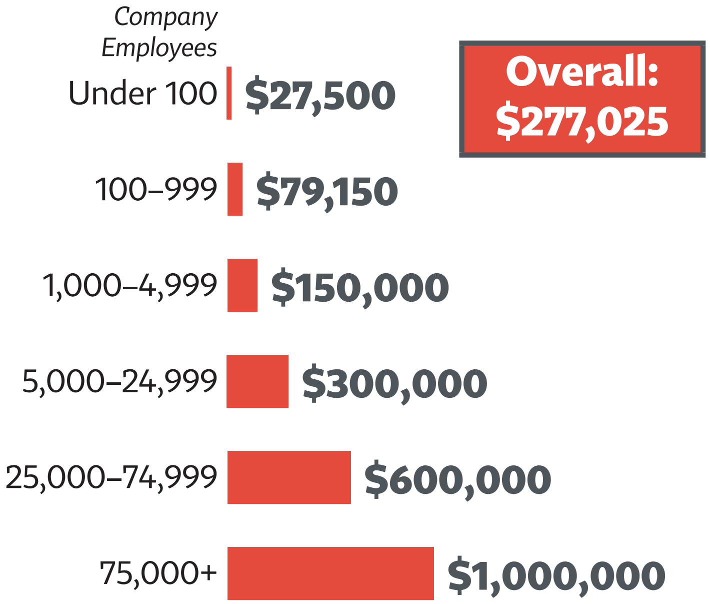
# Not surprisingly, the budget for privacy increases with company size, with an overall average of $277K

- This budget is expected to increase for a third of respondents.

## In Next 12 Months, Expect Privacy Budget Will:



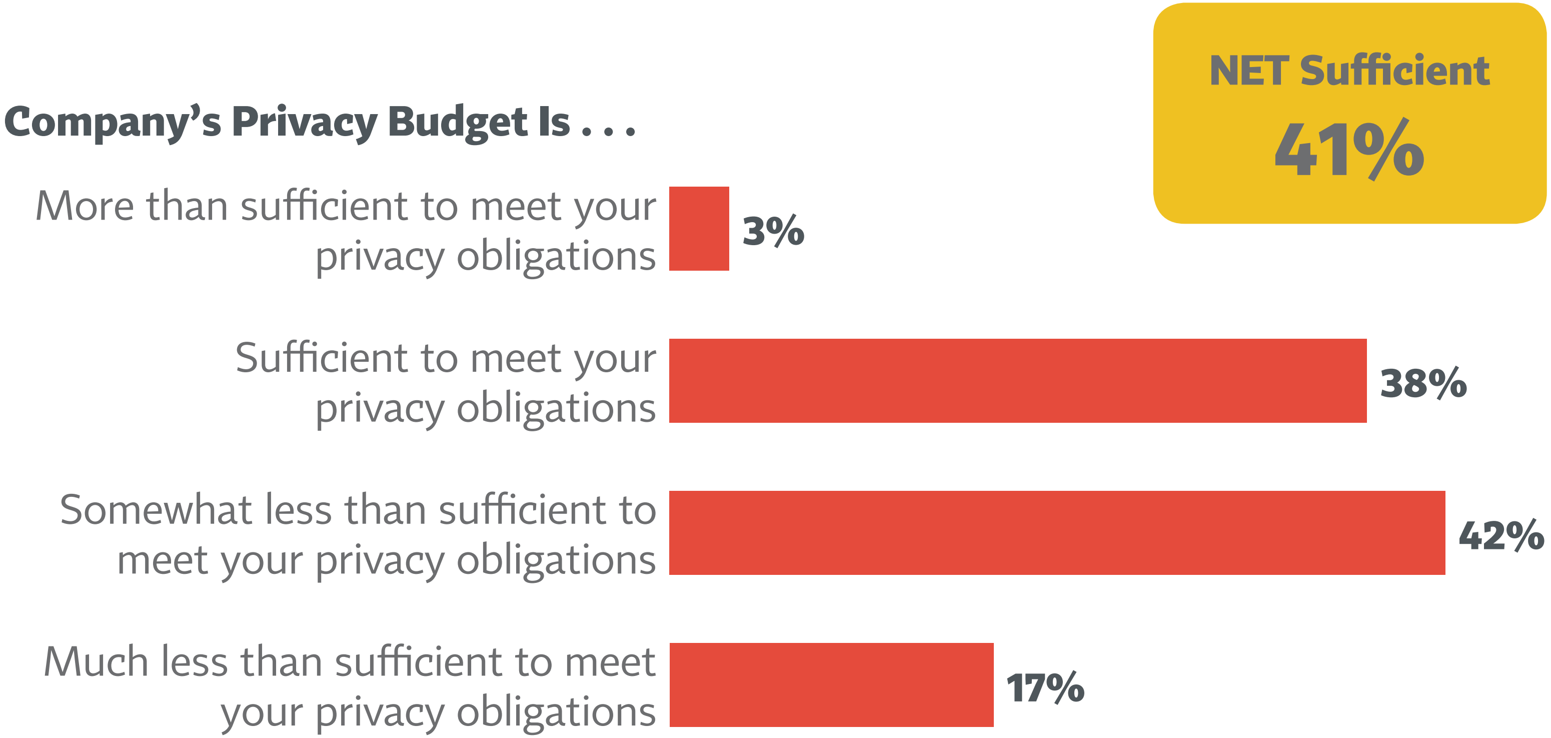
## Privacy Budget by Size of Company



F4: What would you estimate is the approximate budget your company allocates to privacy?
F5: In the next 12 months, you expect your company's privacy budget will …

# Over half of privacy professionals feel their current privacy budget is insufficient

- And nearly one-in-five feel it is **much** less than sufficient to meet their company's privacy obligations

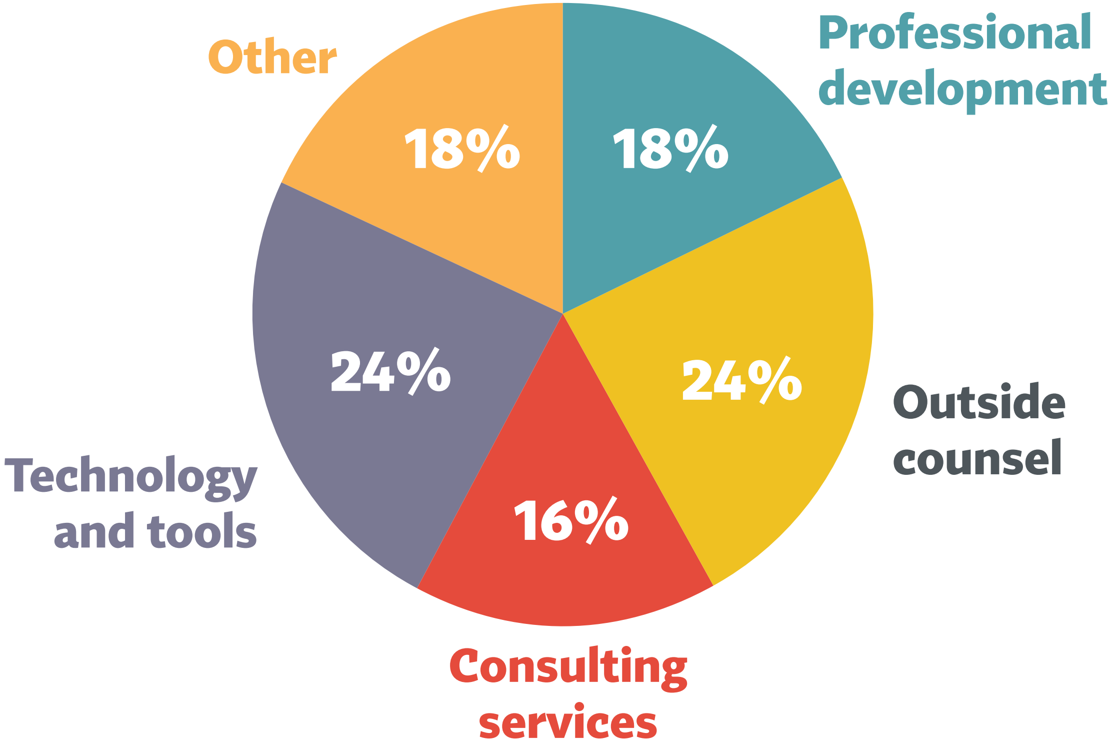


F6: Your company's privacy budget is ...

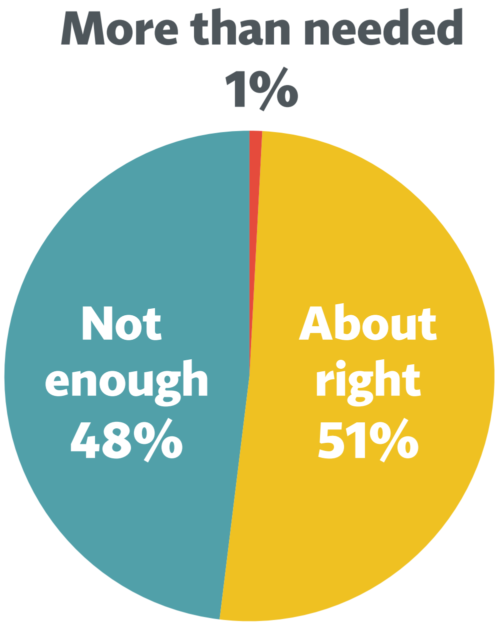
# Salary and travel make up half of the privacy budgets in these organizations

- Opinions are split on whether there is enough spent on privacy training of employees—with nearly half saying it's not enough

## Non-Salary/Travel Budget Components



## Amount Spent on Privacy Training of Employees is . . .

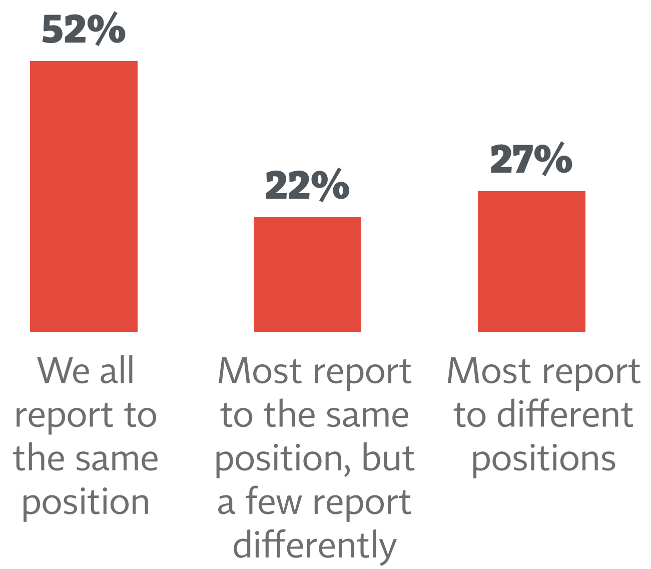


F7: What percent of your company's total privacy budget is allocated to each of the following components?
F8: The amount your company invests on privacy training of its employees is …

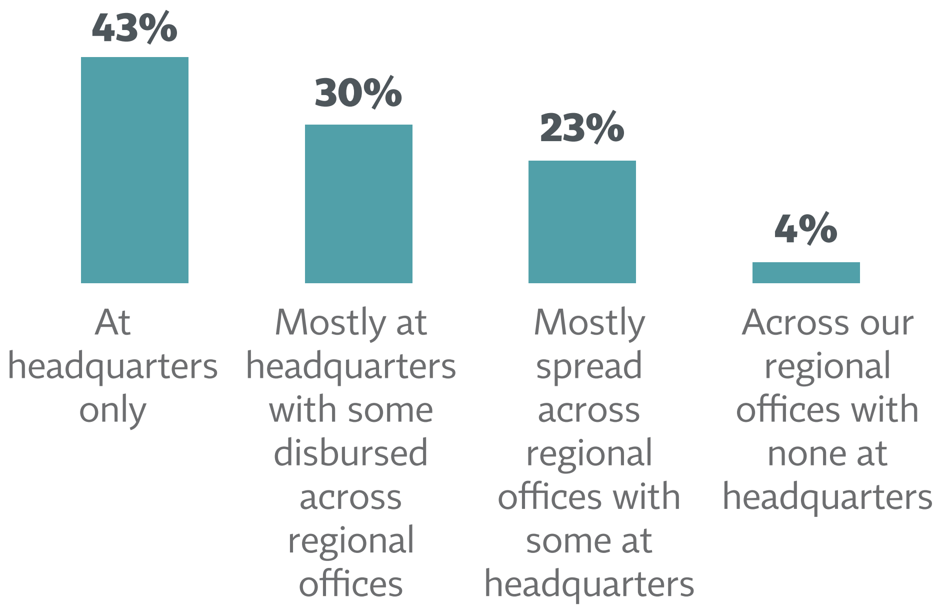
# The privacy function is relatively centralized among these professionals, with all or most reporting to one person

- In addition, privacy personnel are most likely to be based at their company’s headquarters location

## Reporting Structure



## Location of Structure Geographically

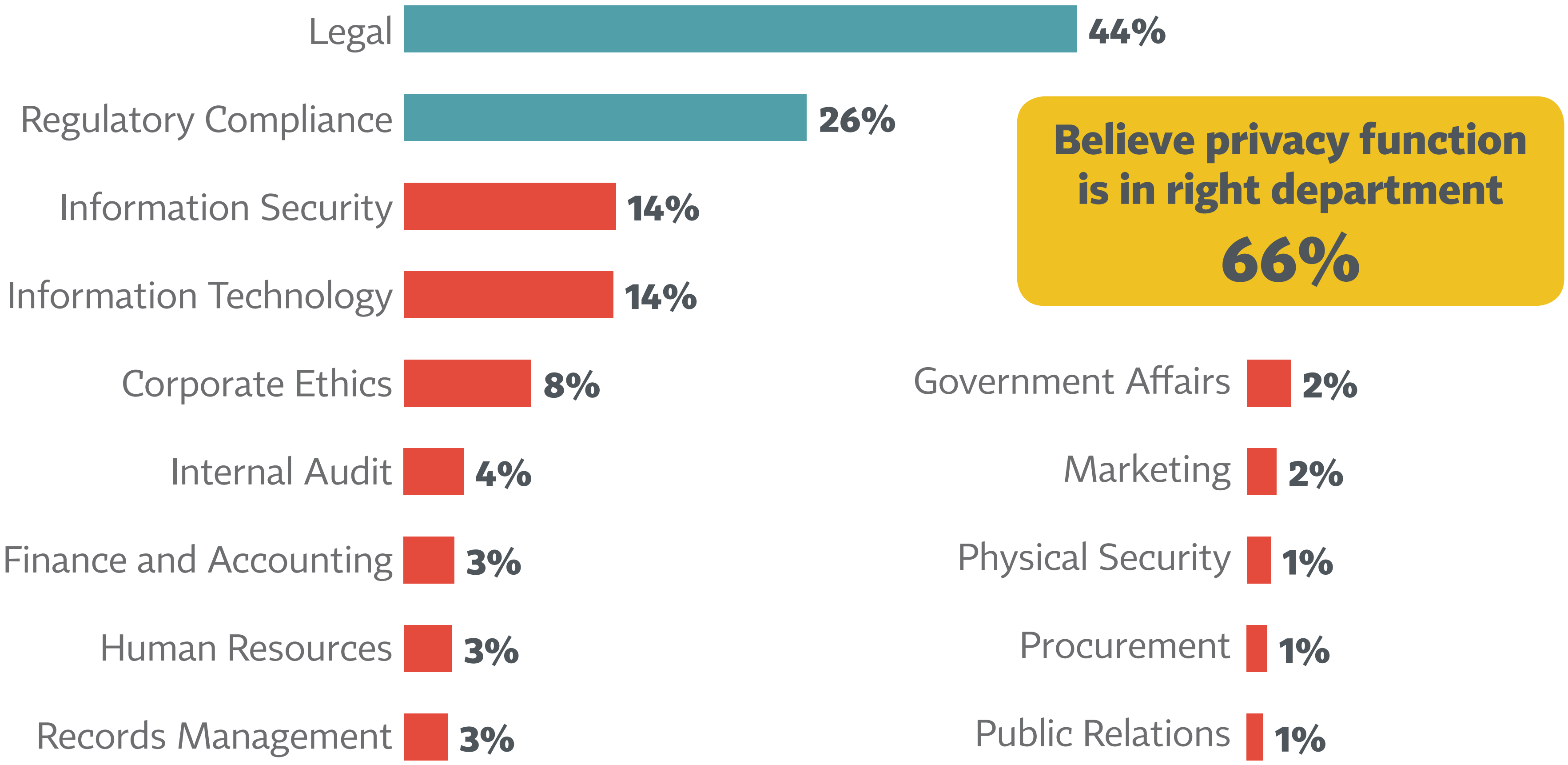


F10: Which of the following best describes the reporting structure for you and the colleagues you work with in privacy?
F11: The privacy function of your company is geographically located ...

# Privacy is far more likely to be housed within the legal department than in any other function

- What's more, two-thirds feel it is located in the right department for their organization

## Location of Structure Within Organization

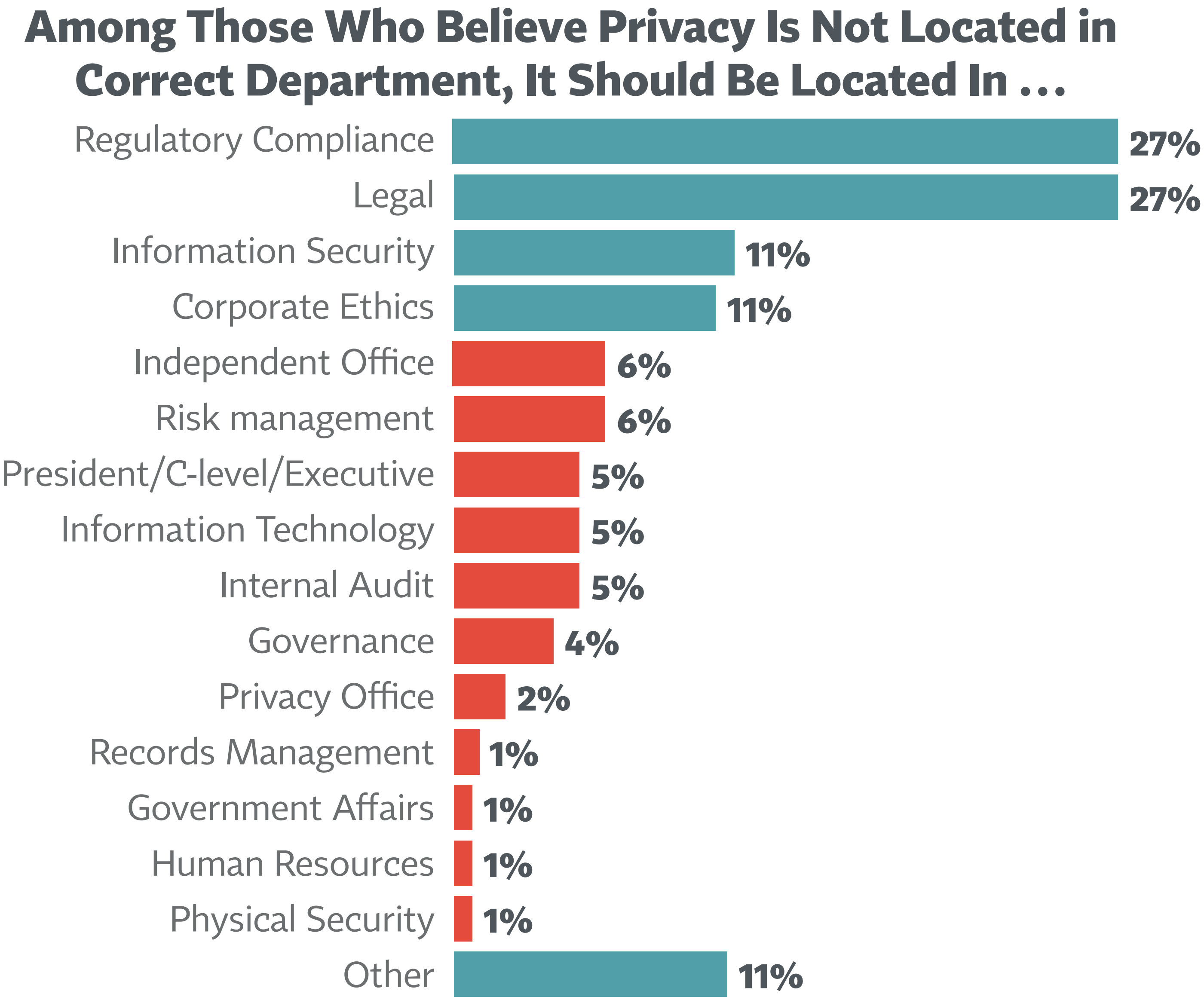


**Believe privacy function is in right department**

**66%**

F12: Where within your company is the privacy function located?
F13: In your opinion, is the privacy function located in the right department?

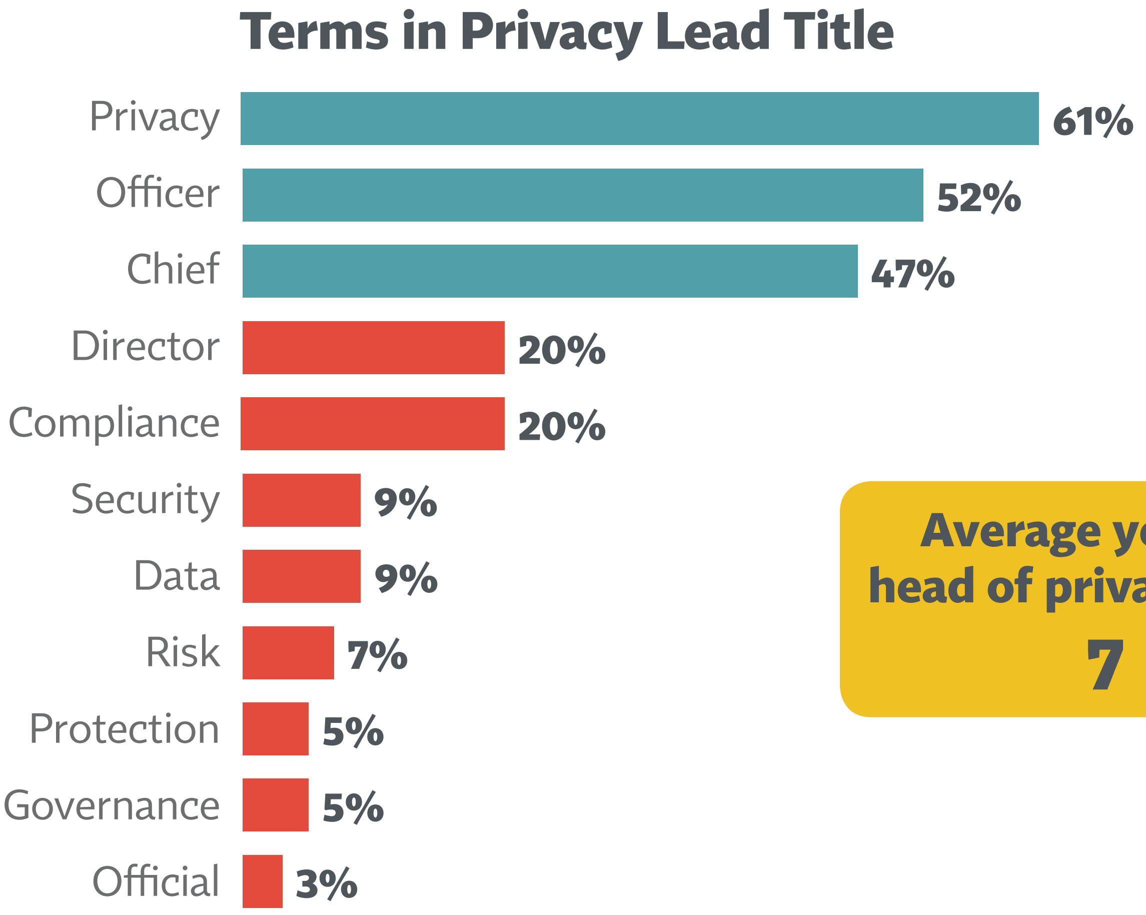
# Among the one-third saying privacy is housed in the *wrong* department, most feel it should be in compliance or legal



F14: Where within your company should the privacy function be located?

# Heads of privacy groups most often have “privacy,” “officer,” and/or “chief” in the title, with a mean tenure of 7 years

- That person most often has a different, but at least equivalent position, to the Chief Information Security Officer, and he or she most likely has other responsibilities outside of privacy



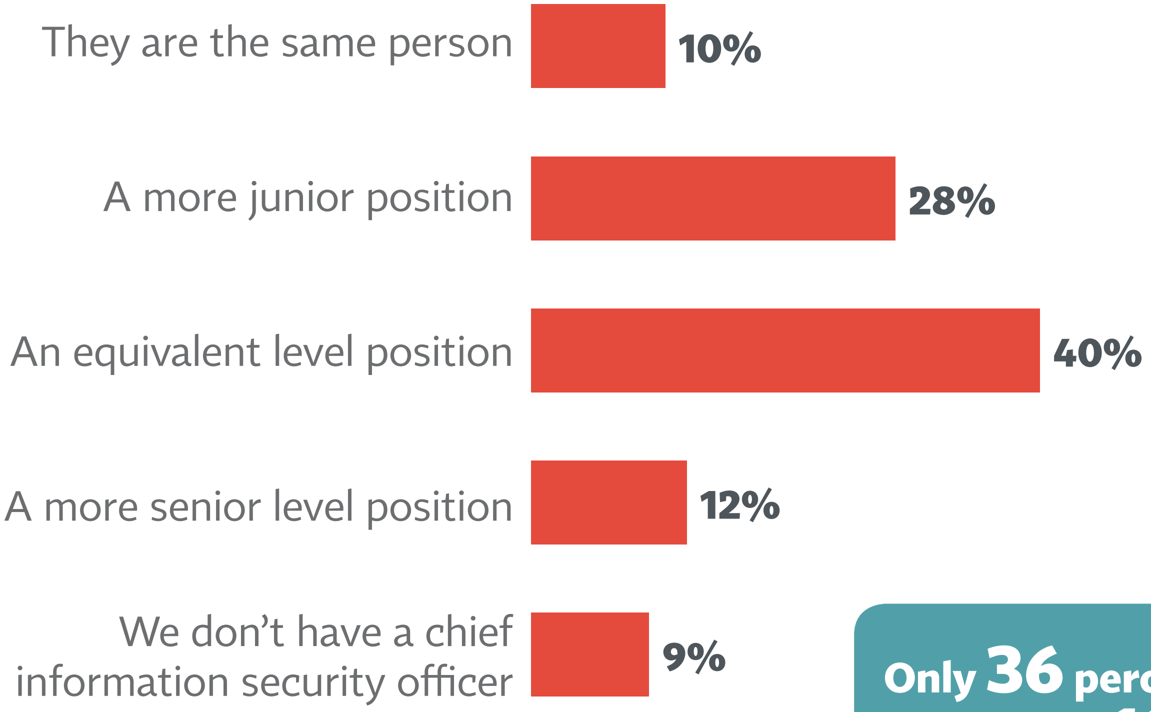
**Average years as head of privacy team:**

**7**

F18: Which of the following words occur in the official, formal title of the person in rung #1 [or Privacy lead from F22]?
F20: For how many years has your company had a privacy leader or chief privacy officer?

# The privacy lead is most often equivalent to the CISO, and usually has other roles

## Compared to Chief Information Security Officer, Privacy Lead Is . . .



**Only 36 percent of privacy leads are dedicated 100 percent to privacy**

F23: How does the privacy leader/chief privacy officer compare with your company's chief information security officer or the highest level information security person in the company? The privacy leader/chief privacy officer is …

F24: Does the individual designated as your company's privacy leader have responsibilities other than privacy?

# Respondents report an average of two rungs above the top privacy lead

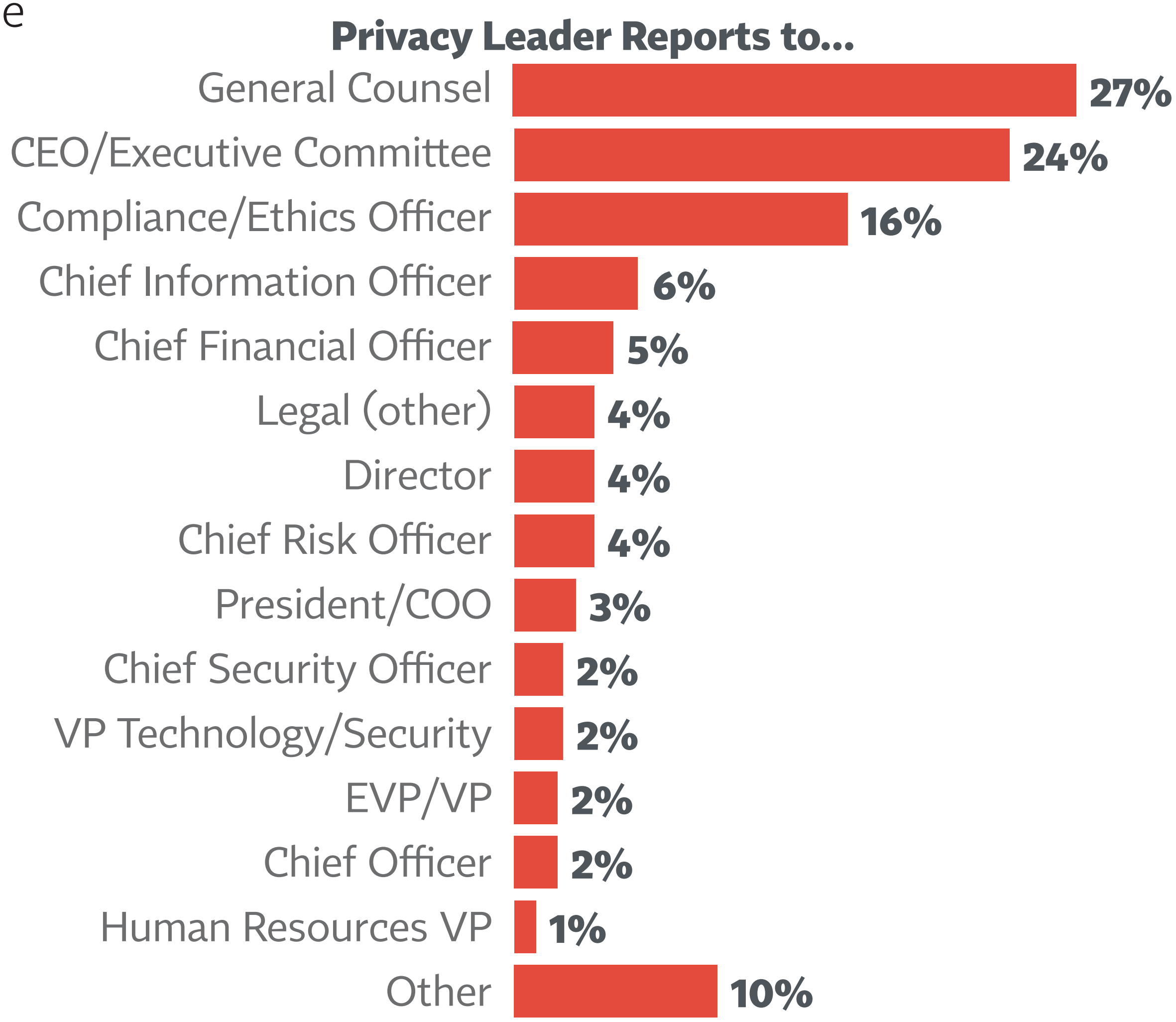
- The privacy lead most often reports to the General Counsel or CEO/Executive Committee

CEO

| Rungs | |
|---|---|
| 0 | 3% |
| 1 | 17% |
| 2 | 34% |
| 3 | 31% |
| 4 | 12% |
| 5 | 3% |
| >5 | 1% |

Privacy Leader or CPO

Median 2 rungs above top privacy position (Mean=3 rungs)



F25: Thinking back to the vertical ladder and now applying it to the company overall, how many rungs (positions) of seniority are there above the top privacy position, up to and including the CEO?

F26: Who does the top privacy person report to?

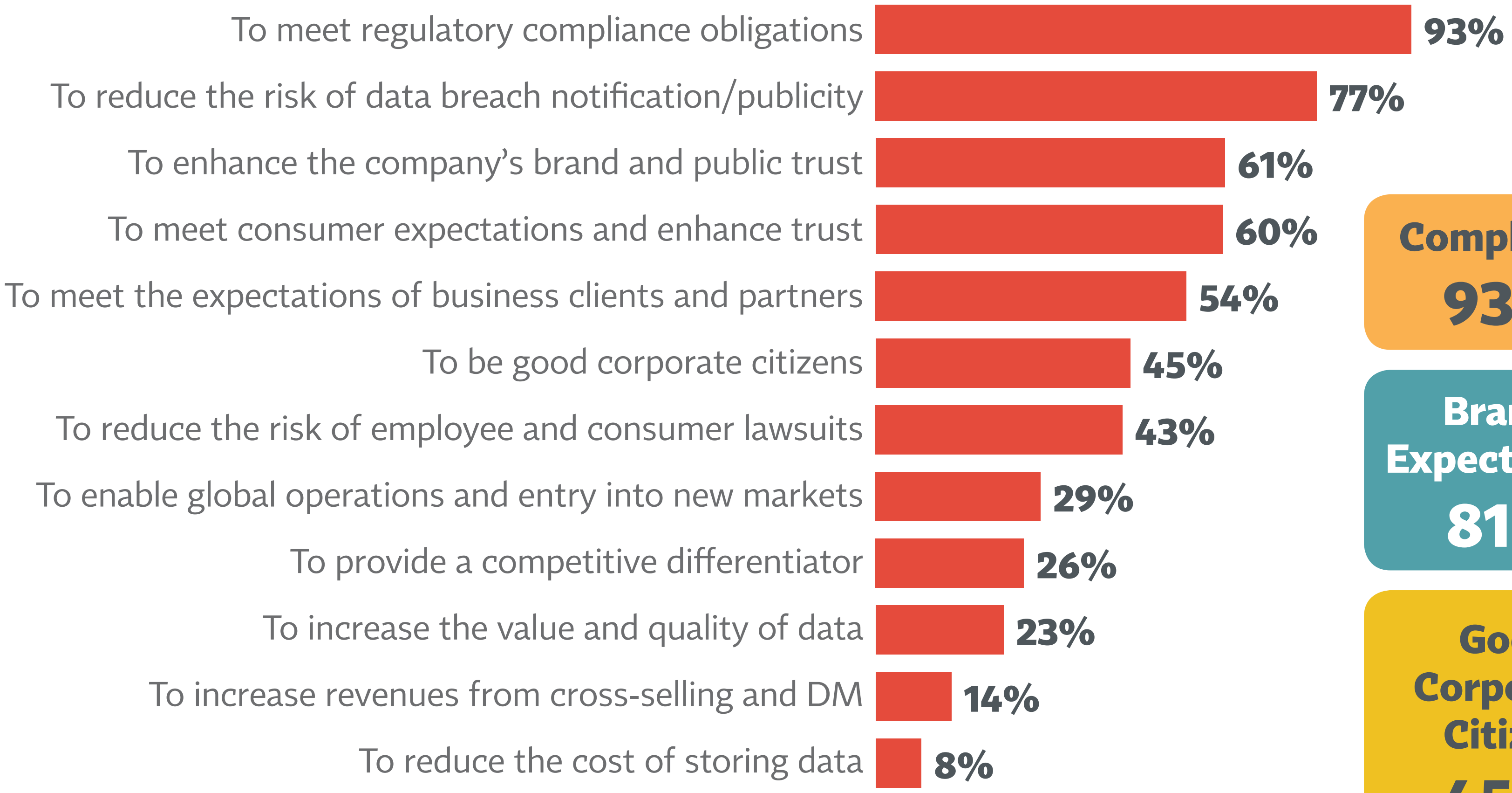
# 3 Privacy Group Characteristics

- Privacy Group Characteristics: Structure
- **Privacy Group Characteristics: Responsibilities**
- Privacy Group Characteristics: Privacy Function in the Business Context
- Privacy Group Characteristics: Internal and External Resources

# Regulatory compliance is the number one reason these organizations have a privacy function

- Not far behind is reducing the risk of embarrassing, breach-related publicity
- However, the benefits of a strong privacy function, in particular for enhancing public and consumer trust, are frequently cited reasons, as well

## Main Reasons for Having Privacy Function



Compliance 93%

Brand/ Expectations 81%

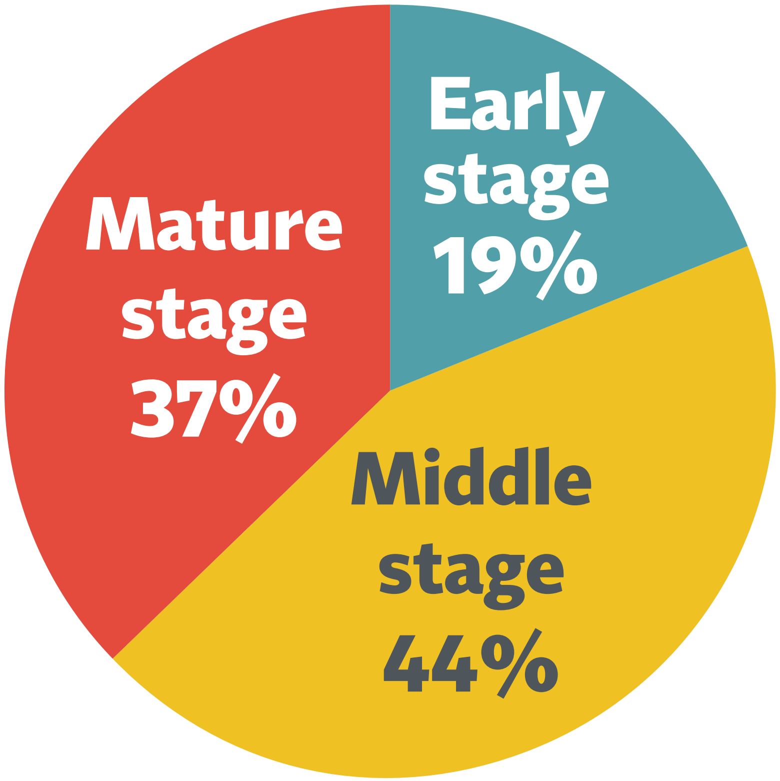
Good Corporate Citizen 45%

E6. Which of the following would you say are the main reasons that the leadership of your company supports and funds a privacy function?

# On average, these organizations have had a privacy program for 7 years

- Professionals are most likely to characterize their company as in the "middle stage" of the privacy program lifecycle, although 37% say they're in the "mature stage"

## Where in Privacy Maturity Process Is Company?



**Mean Number of Years with Privacy Program**

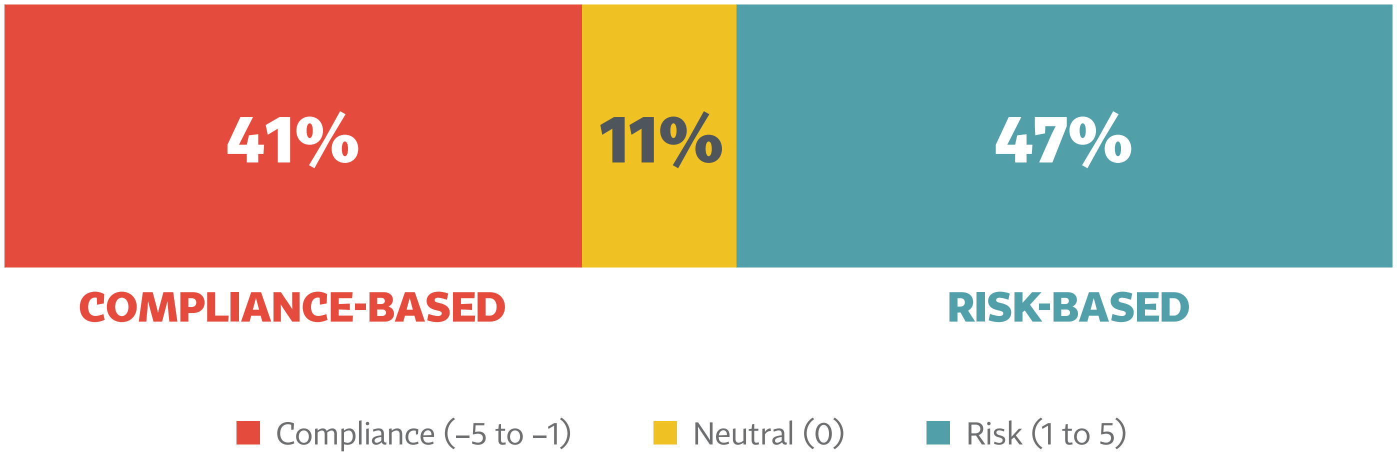
**7**

E1. Please select the maturity stage of your company's privacy program.
E2. For how many years has your company had a dedicated privacy program?

# These firms are nearly equally divided between having a compliance-based vs. risk-based approach to privacy

- We'll see later that this distribution differs by level of privacy maturity, however, with early-stage firms more likely to be focused on compliance, and mature firms focused more on risk management

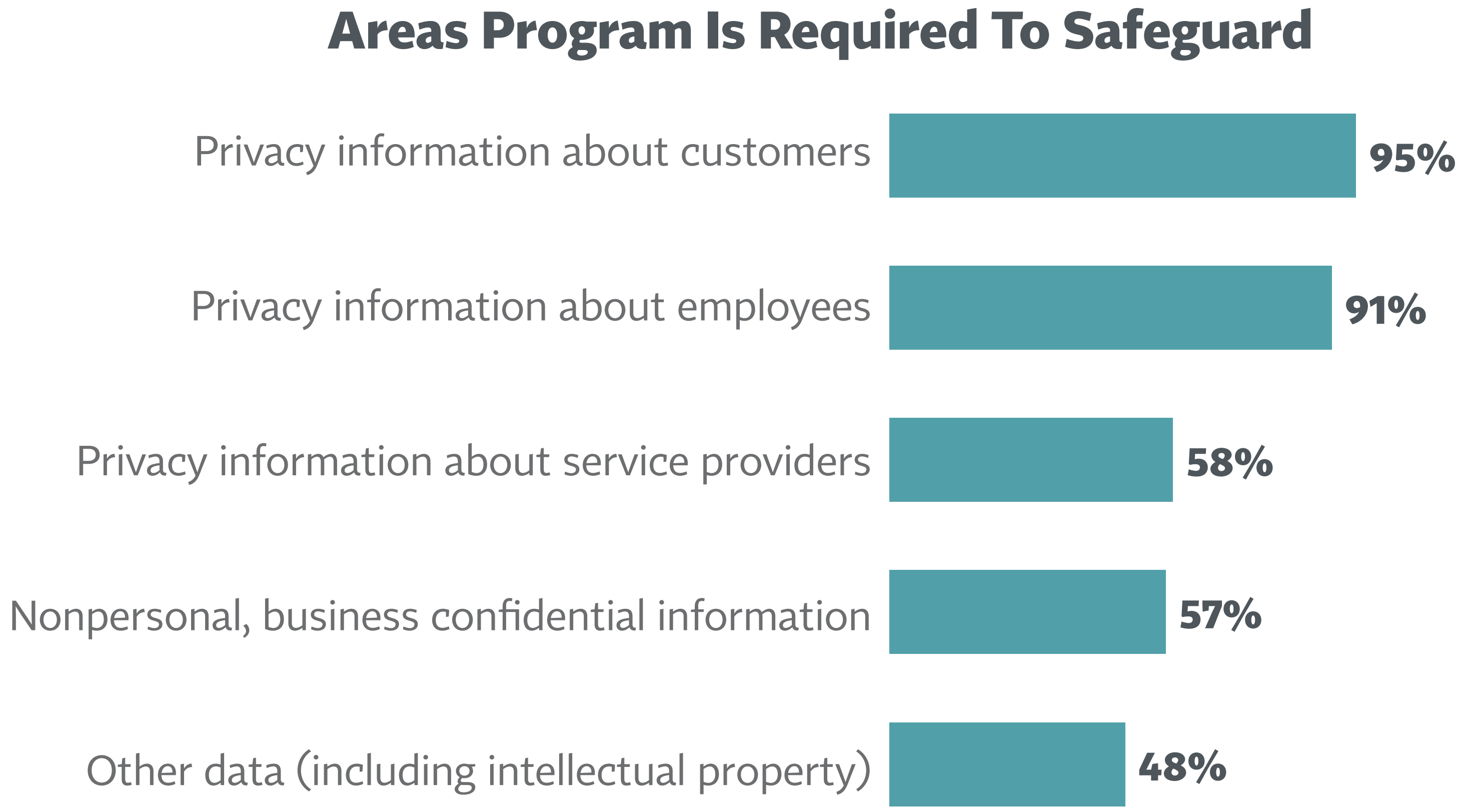
## Compliance vs. Risk Approach to Privacy



E8. Please use the slider below to indicate where your company falls on this spectrum between compliance-based or risk-based.

# Nearly all privacy programs are required to focus on customer and employee information

- However, more than half also have responsibilities for service provider information and for information about the business itself

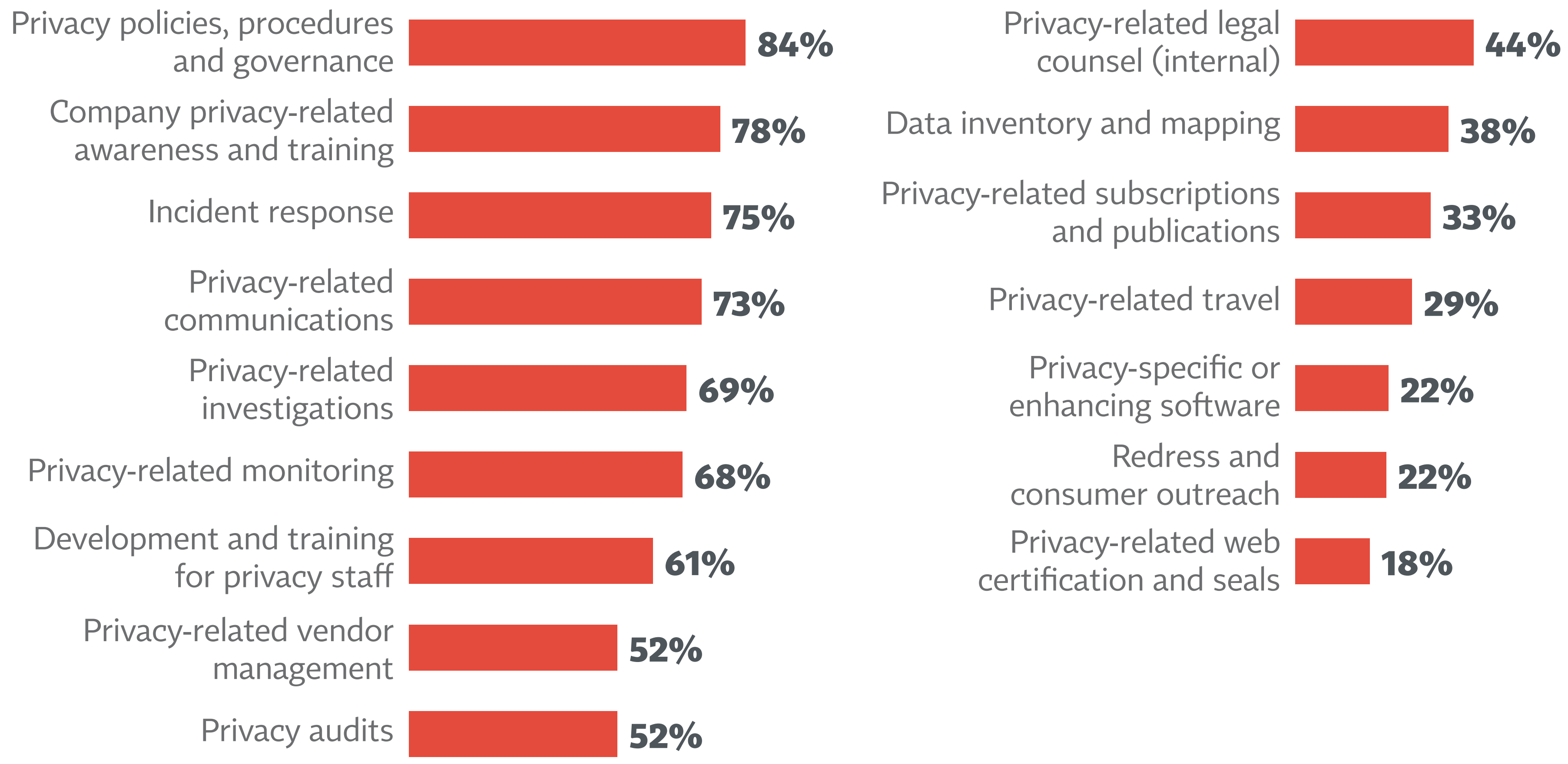


E4. What types of information is your privacy program required to safeguard?

# As we saw with distribution of work time, these privacy programs cover a broad range of responsibilities

- Policies and procedures, awareness and training, incident response and communications are at the top of a very long list of tasks

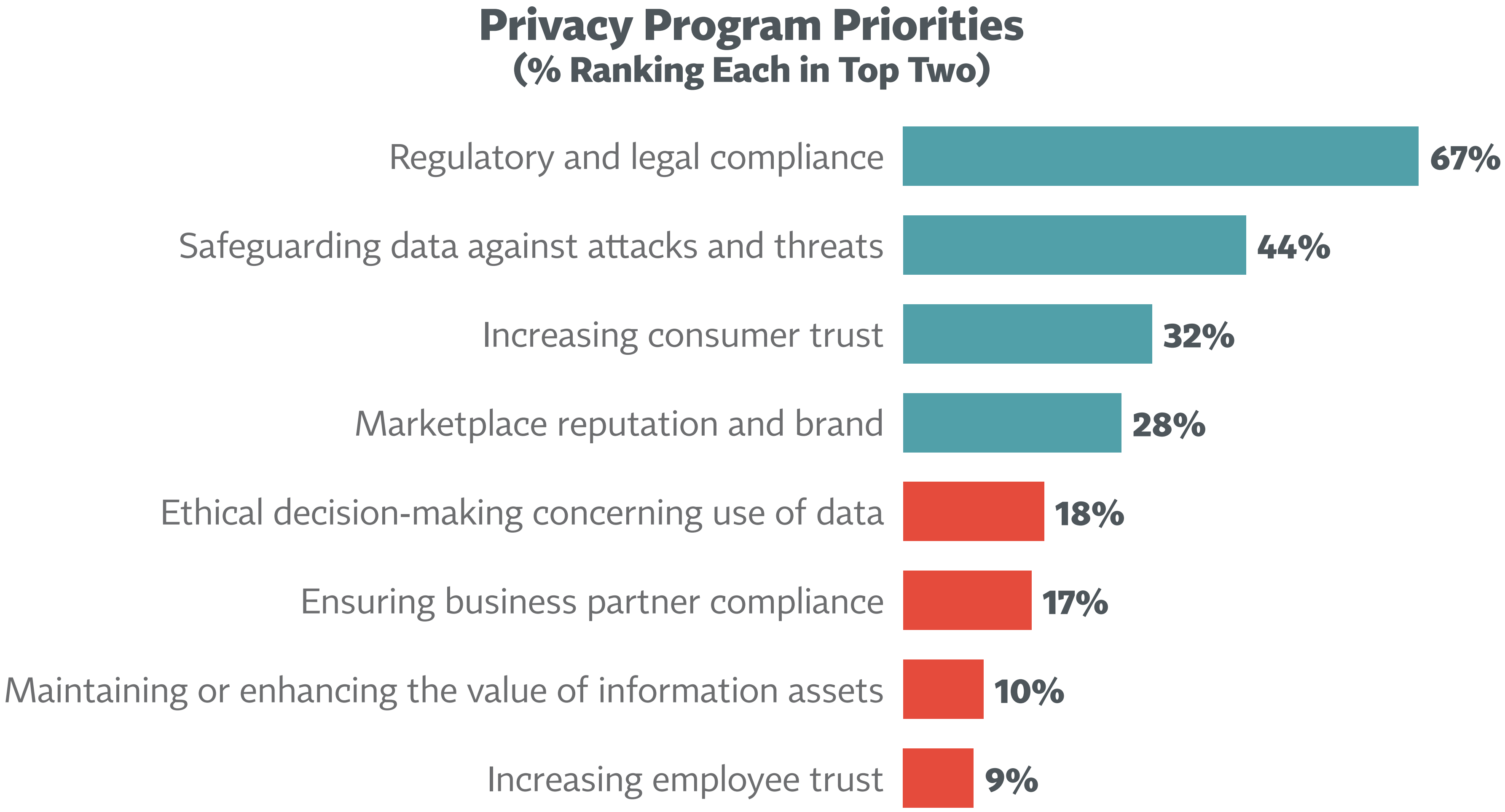
## Areas of Annual Responsibility



D5. Which of the following is your team responsible for accomplishing on an annual basis?

# When professionals are asked to prioritize their programs' responsibilities, compliance rises to the top

- Protection against data breaches falls next, followed by two more "proactive" tasks—increasing consumer trust and enhancing brand image



E5. Please rank these priorities from 1 = highest to 8 = lowest for your company. Do not assign any rank for a priority that is not applicable to your company.

# 3 Privacy Group Characteristics

- Privacy Group Characteristics: Structure
- Privacy Group Characteristics: Responsibilities
- **Privacy Group Characteristics: Privacy Function in the Business Context**
- Privacy Group Characteristics: Internal and External Resources

# These are the areas with which privacy works

- Including data on how important they feel it is to work with these teams, how much influence over them they have and whether they feel they should have more influence over these areas

## Functional Areas Privacy Works With

| | | |
|---|---|---|
| **Top Functional Areas Privacy Works With** | Information Security | 83% |
| | Legal | 79% |
| | Information Technology | 72% |
| | Regulatory Compliance | 64% |
| | Human Resources | 56% |
| **Second Tier of Functional Areas Privacy Works With** | Internal Audit | 45% |
| | Marketing | 42% |
| | Product Managers | 40% |
| | Records Management | 39% |
| | Procurement | 34% |
| | Physical Security | 31% |
| | Corporate Ethics | 30% |
| | Sales | 26% |
| | Product Designers | 25% |
| | Public Relations | 25% |
| **Functional Areas Privacy Is Least Likely to Work With** | Product Engineers | 24% |
| | Government Affairs | 24% |
| | Finance and Accounting | 23% |
| | Mergers and Acquisitions | 15% |
| | Supply Chain and Logistics | 12% |

# When they’re asked about the importance of working with different groups, the same areas rise to the top

- Professionals feel that cooperation with IS, legal, IT, compliance and HR are the highest priorities for the privacy function

## Importance of Cooperation for Privacy Goals, By Function

| | | |
|---|---|---|
| **Cooperation for Privacy Goals Is Most Important** | Information Security | 80% |
| | Legal | 75% |
| | Information Technology | 63% |
| | Regulatory Compliance | 62% |
| | Human Resources | 41% |
| **Cooperation for Privacy Goals Is Somewhat Important** | Corporate Ethics | 35% |
| | Records Management | 34% |
| | Internal Audit | 32% |
| | Product Managers | 31% |
| | Marketing | 31% |
| | Product Designers | 30% |
| | Product Engineers | 28% |
| **Cooperation for Privacy Goals Is Least Important** | Procurement | 23% |
| | Physical Security | 22% |
| | Government Affairs | 21% |
| | Public Relations | 15% |
| | Sales | 15% |
| | Finance and Accounting | 13% |
| | Mergers and Acquisitions | 13% |
| | Supply Chain and Logistics | 8% |

# One-third to one-half of professionals say they want more influence over a number of key departments

- Product functions stand out as areas where desired influence is relatively high, and actual incidence is lower than for comparable functions

## Influence vs. Desired Influence Over Functions

| | Currently Has Great Deal/Some Influence | Should Have Great Deal/Somewhat More Influence |
|---|---|---|
| Information Security | 87% | 46% |
| Regulatory Compliance | 85% | 37% |
| Information Technology | 81% | 46% |
| Human Resources | 73% | 41% |
| Corporate Ethics | 70% | 41% |
| Records Management | 66% | 33% |
| Product Managers | 56% | 37% |
| Product Designers | 53% | 38% |
| Product Engineers | 51% | 36% |

G3: For each of these same functions, please indicate whether privacy leaders have a great deal of influence over the operations of the function, some influence, little influence or no influence over the operations and budget of the function within your organization.

# Three other functions are also areas with relatively low influence, but a relatively strong desire for more

- Those areas are: procurement, government affairs and physical security

## Influence vs. Desired Influence Over Functions

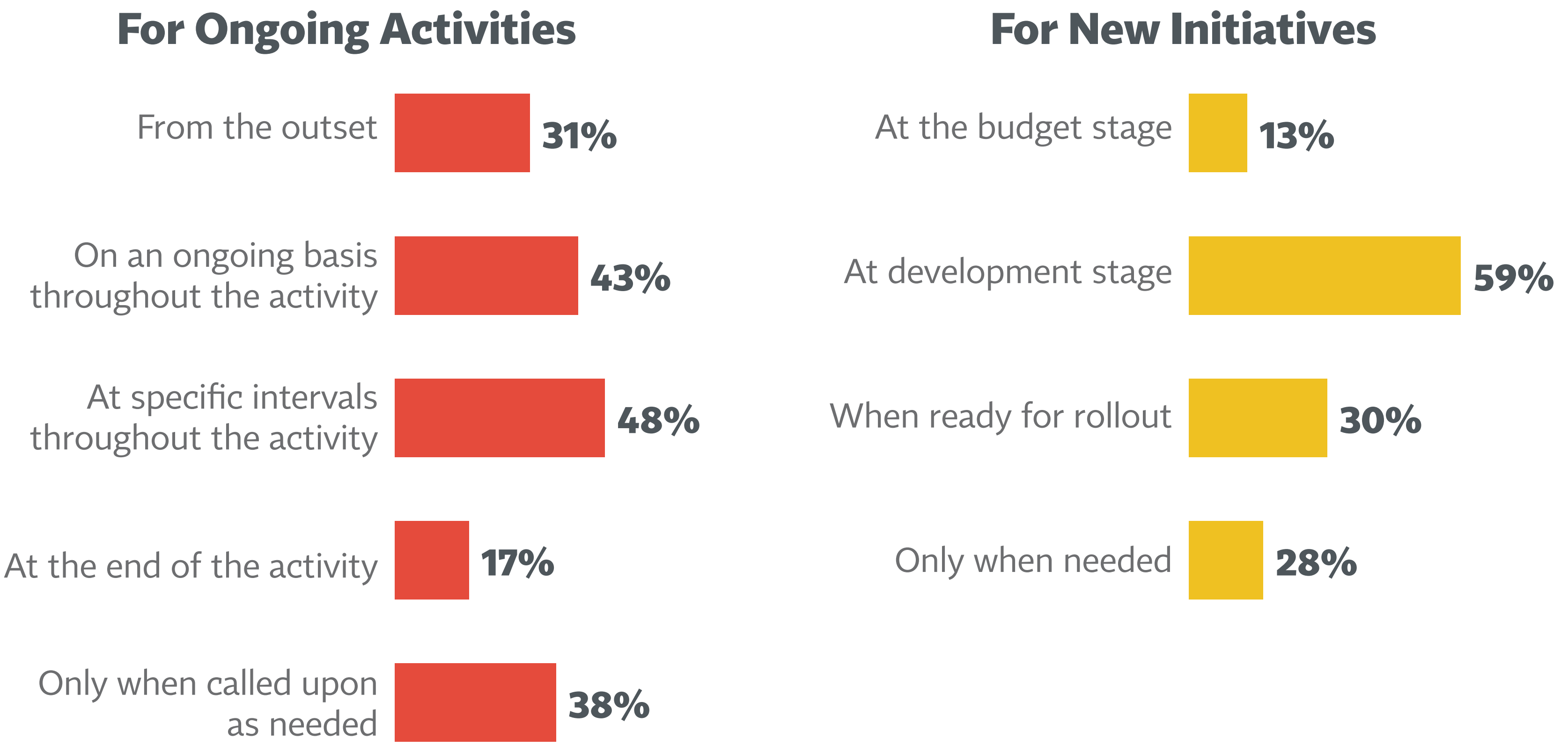
| | Currently Has Great Deal/Some Influence | Should Have Great Deal/Somewhat More Influence |
|---|---|---|
| Legal | 83% | 32% |
| Internal Audit | 65% | 32% |
| Procurement | 54% | 30% |
| Government Affairs | 55% | 30% |
| Physical Security | 58% | 29% |
| Sales | 36% | 27% |
| Mergers and Acquisitions | 37% | 26% |
| Finance and Accounting | 36% | 25% |
| Public Relations | 50% | 24% |
| Supply Chain and Logistics | 29% | 21% |

G4: For this same list, please indicate whether you feel that privacy leaders should have a great deal more influence, somewhat more influence, a little more influence or no more influence than you currently have over the operations.

# 4-5 in 10 professionals say that privacy tends to be involved throughout ongoing activities

- However, nearly 40% say they're only involved when needed
- For brand-new initiatives, 59% say they're involved at the development stage of the project (although another 28% say only when called on)

## When in Process Is Privacy Involved?



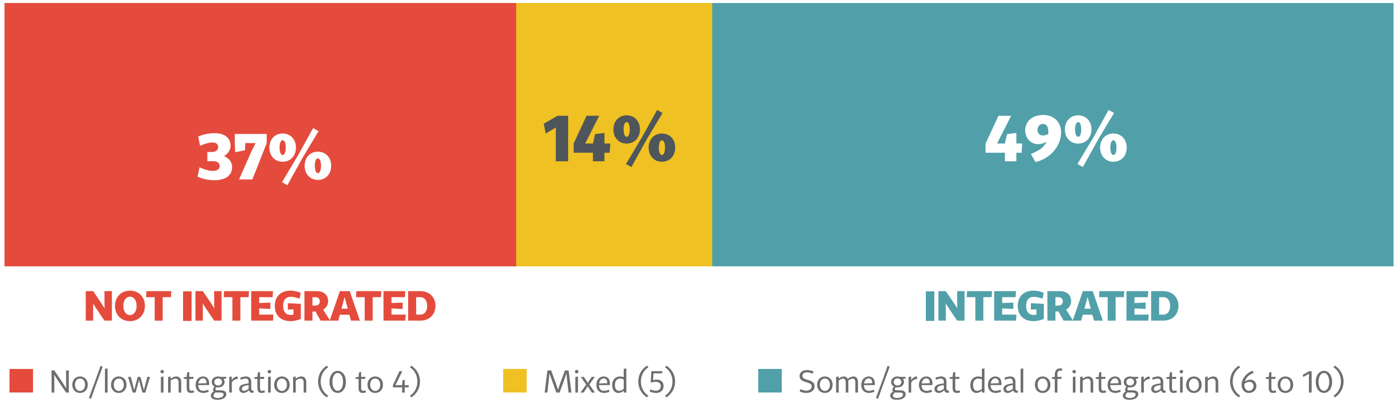
G5: In a general sense, for ongoing activities within your company that may involve privacy-related information, representatives of the privacy function are involved …

G6: Now thinking about new projects or initiatives established by your company that may involve privacy-related information, representatives of the privacy function are involved …

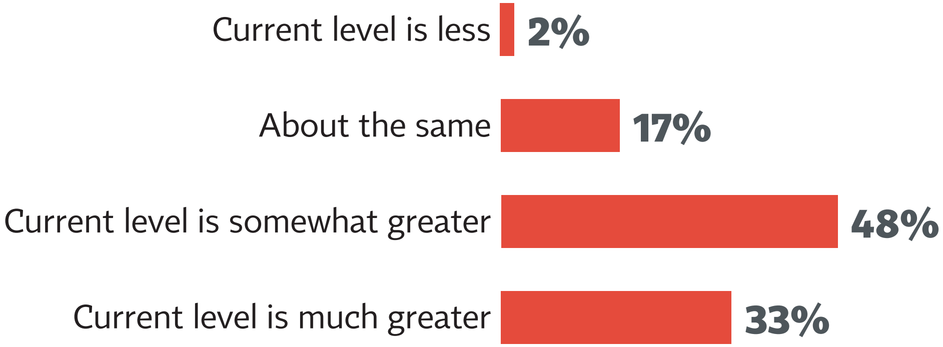
# About half of professionals give positive ratings to how integrated privacy is with company initiatives

- And strong majorities say the level of integration has increased over the past few years, including one-third who say it's now MUCH greater

## Privacy Integration in Planning and Implementation



## Current Integration Level vs. a Few Years Ago



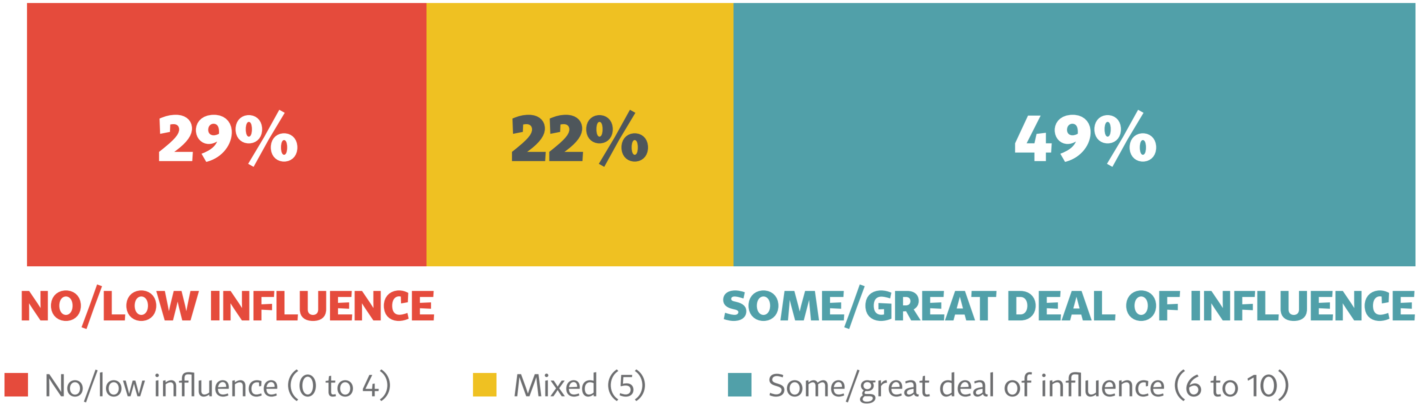
G7: To what extent would you say those in the privacy function of your company are integrated into the planning and implementation of initiatives that involve privacy-related information?

G8: This level of integration is …

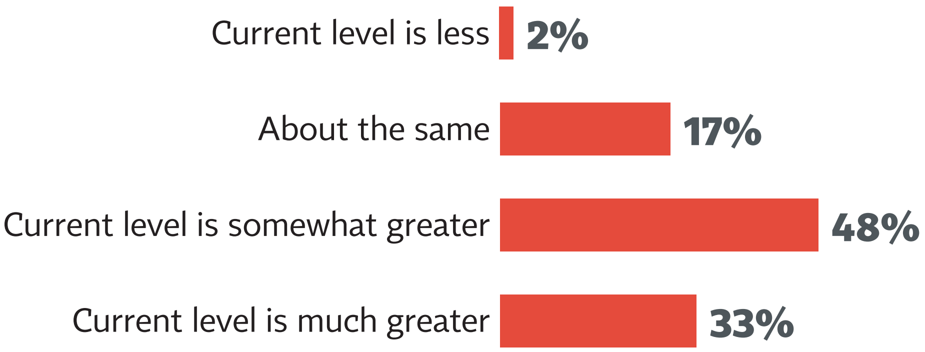
# A similar one-half give positive ratings to the general level of privacy influence over initiatives

- And a majority again say that the level of influence has grown in the past several years

## Privacy Influence on Planning and Implementation



## Current Influence Level vs. a Few Years Ago



G9: How would you describe the degree of influence those in the privacy function of your company have over planning and implementation of initiatives?

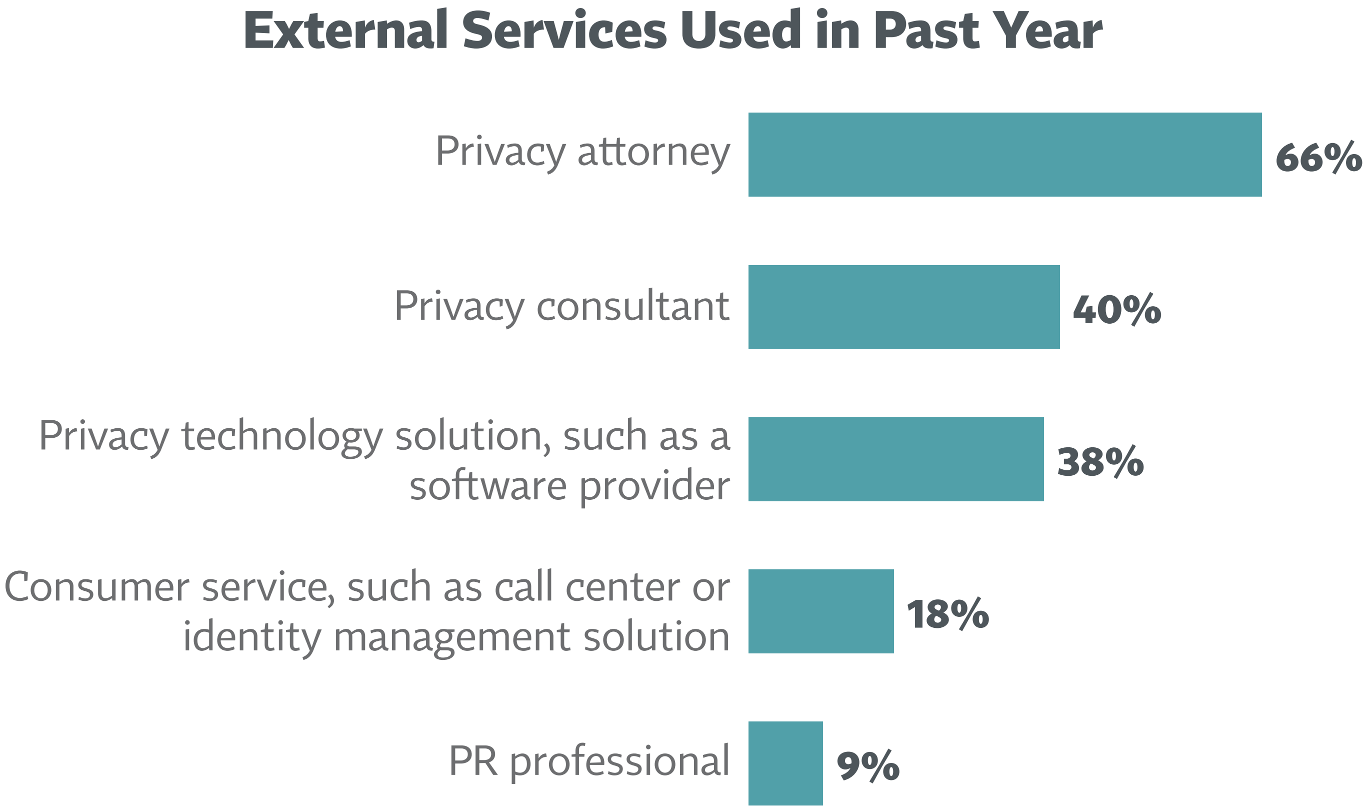
G10: This level of influence is ...

# 3 Privacy Group Characteristics

- Privacy Group Characteristics: Structure
- Privacy Group Characteristics: Responsibilities
- Privacy Group Characteristics: Privacy Function in the Business Context
- **Privacy Group Characteristics: Internal and External Resources**

# The most commonly used external service among privacy professionals is an outside privacy attorney

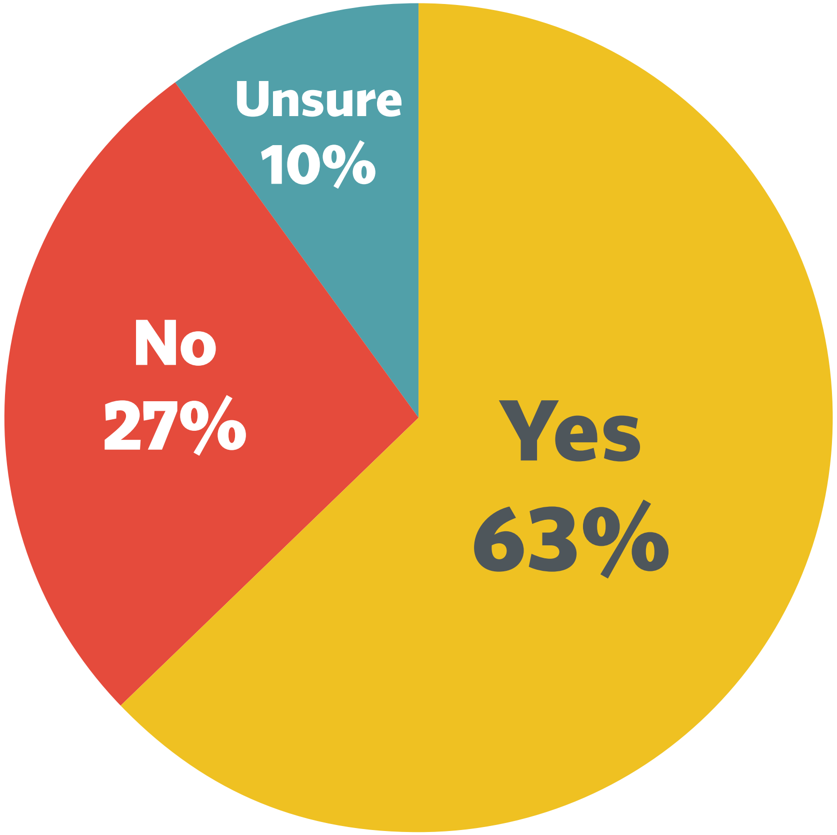
- Privacy consultants and technology solutions were used by 4 in 10; much fewer have used a consumer service or a PR professional



H1: Which of the following external privacy services have you worked with directly within the past year?

# About two-thirds of privacy pros use internal privacy audits

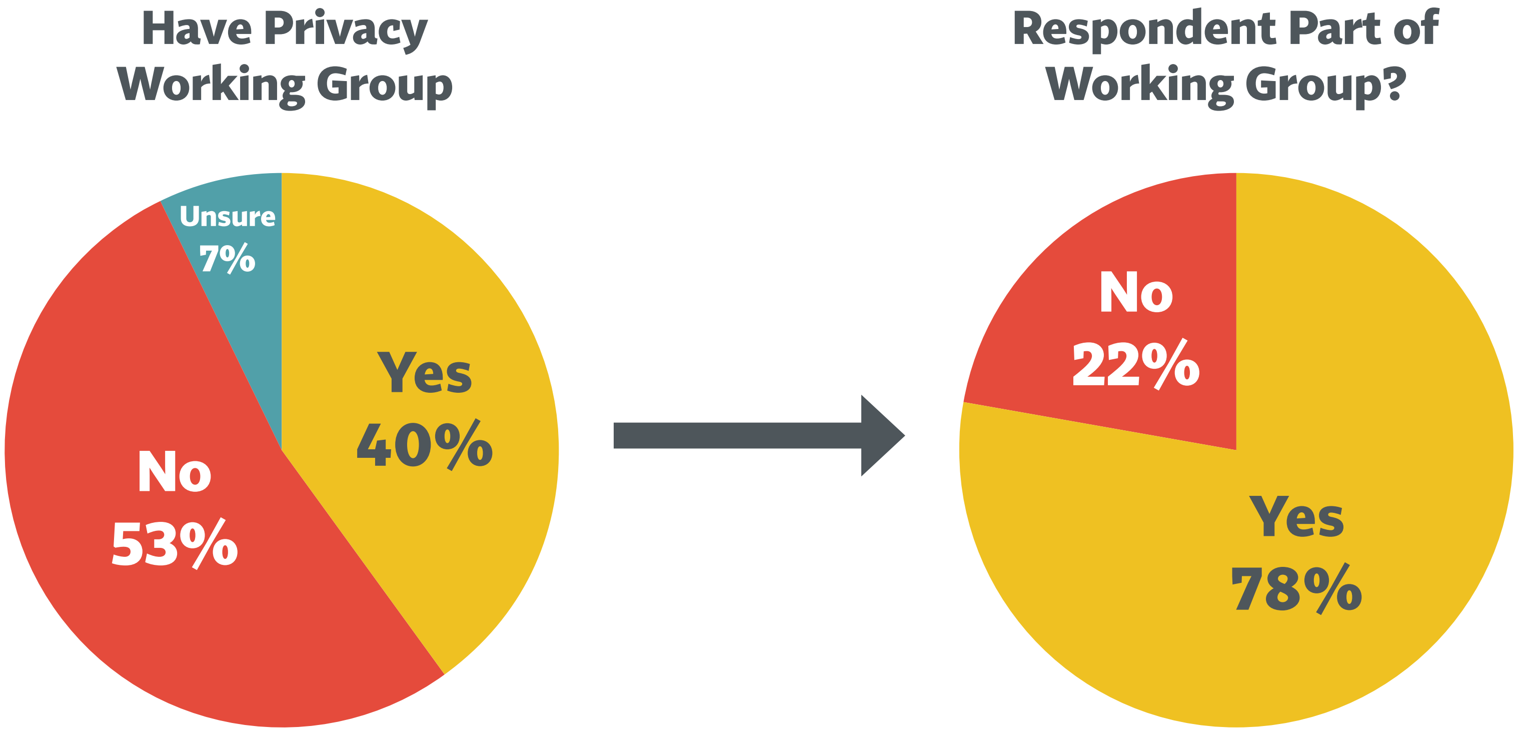
## Use of Internal Audit for Privacy



H2: Does your company use internal audit for privacy audits?

# Respondents split evenly on use of privacy working groups

- Among those who do use them, the survey respondent is typically a group member



H3: Does your organization have a committee of executives ("privacy working group") from a cross section of departments that regularly oversees the privacy office's activities?

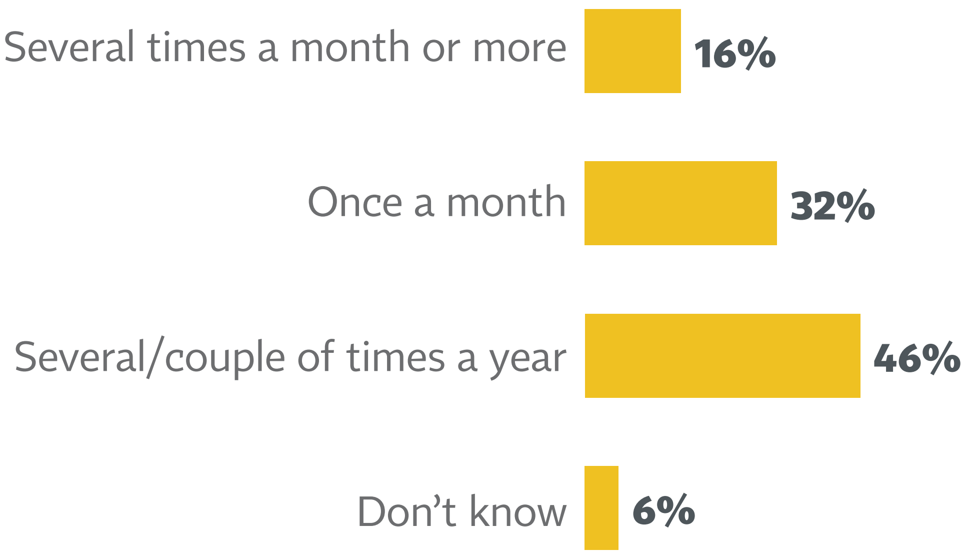
H4: Are you part of the privacy working group?

# The most common privacy working group scenario: meet several times a year…

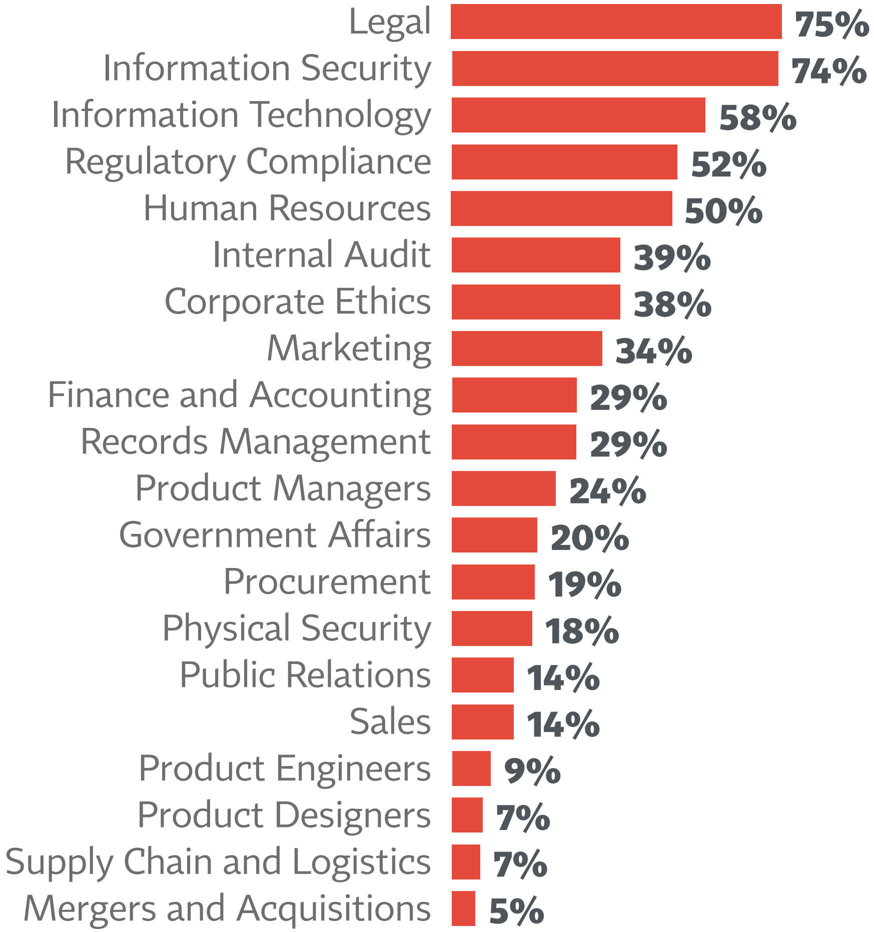
- …With representation from legal, IS, IT, compliance and HR

## Among Those With Privacy Working Group

### How Often Meet



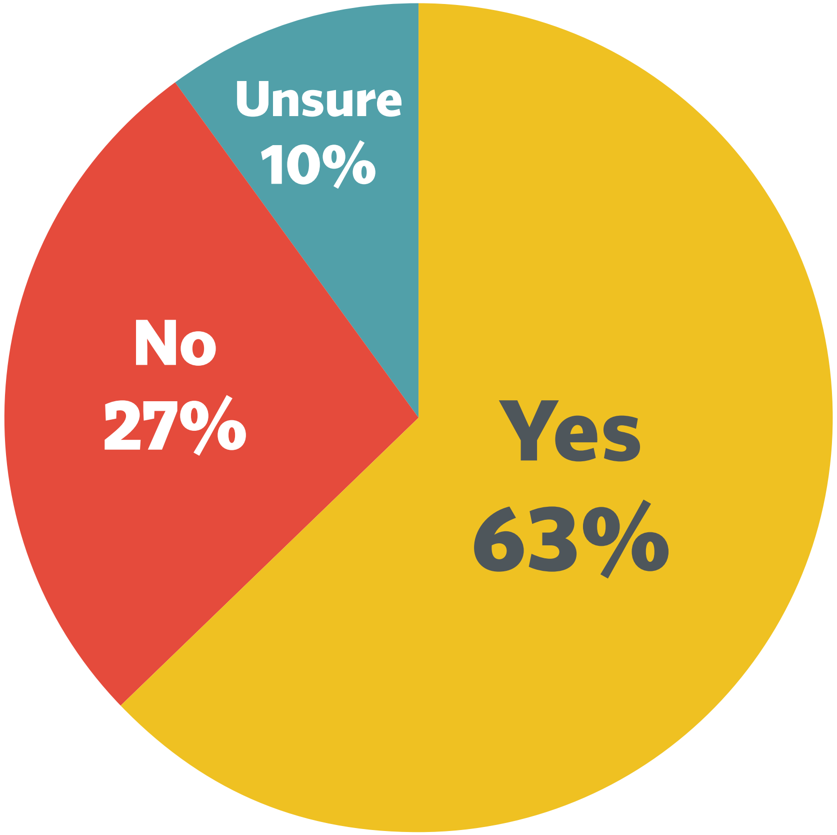
### Functions Represented



H5: How often does this working group meet?
H6: What departments are represented as part of the privacy working group?

# Two-thirds say they have a privacy-related vendor management program in place

## Have Vendor Management Program

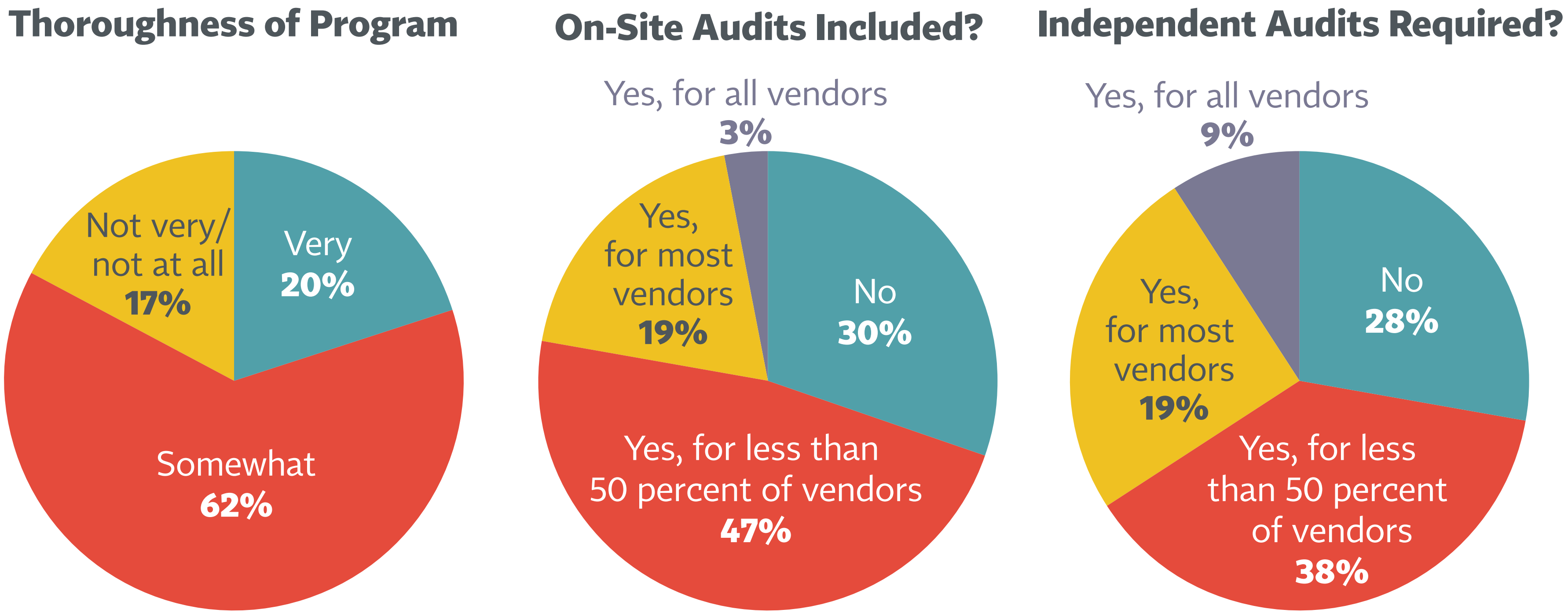


H7: Does your company have a vendor management program designed to ensure the privacy and/or security practices of vendors will not threaten the integrity of your company's privacy standards?

# Current vendor management programs don't receive especially stellar reviews

- Most consider these programs only somewhat thorough, and pluralities say audits apply to fewer than 50% of vendors

## Among Those With Vendor Management Program

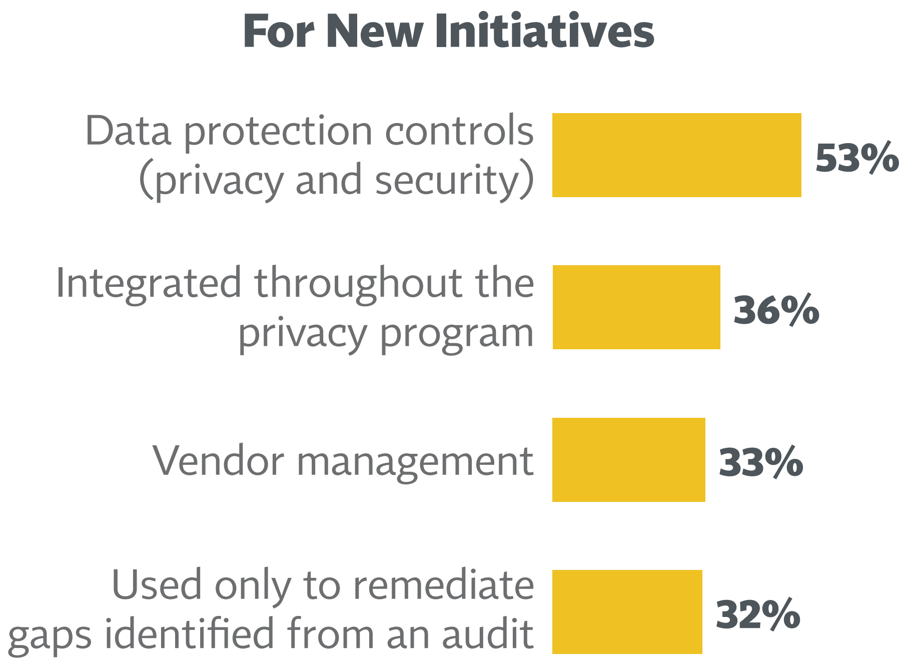


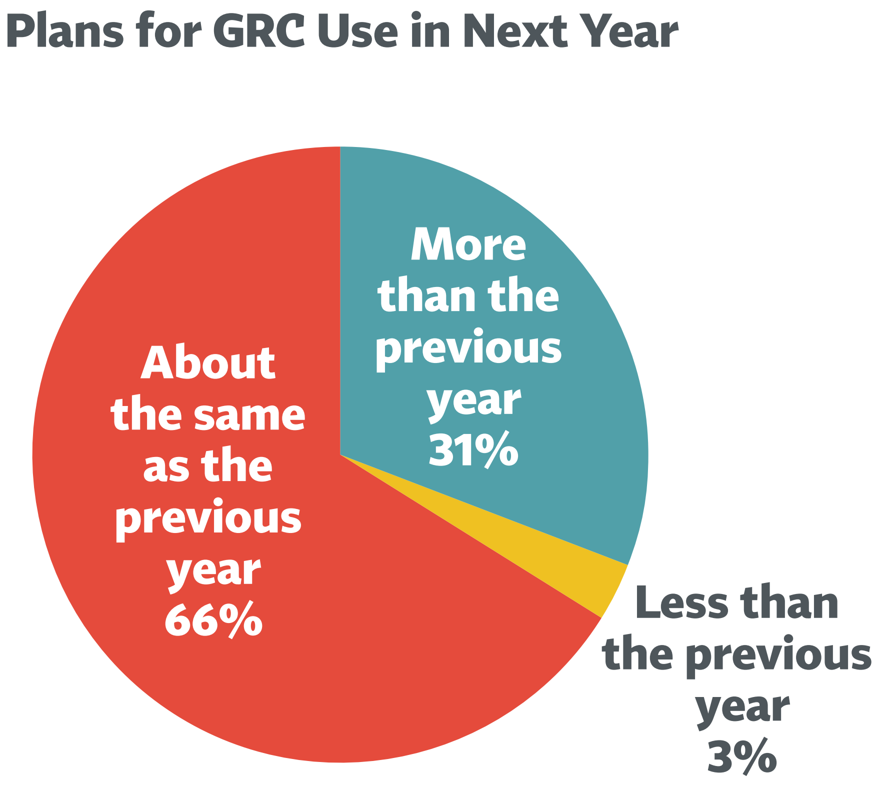
H8: How would you describe this vendor management program?
H9: Does your vendor management program include on-site audits by your company's internal resources?
H10: Does your vendor management program require independent audit reports of privacy and security from vendors?

# Data protection controls are the most common GRC tool used

- Although most say their use of GRC won't change in the coming year, 31% say it will increase

## Among Those Using GRC Tools

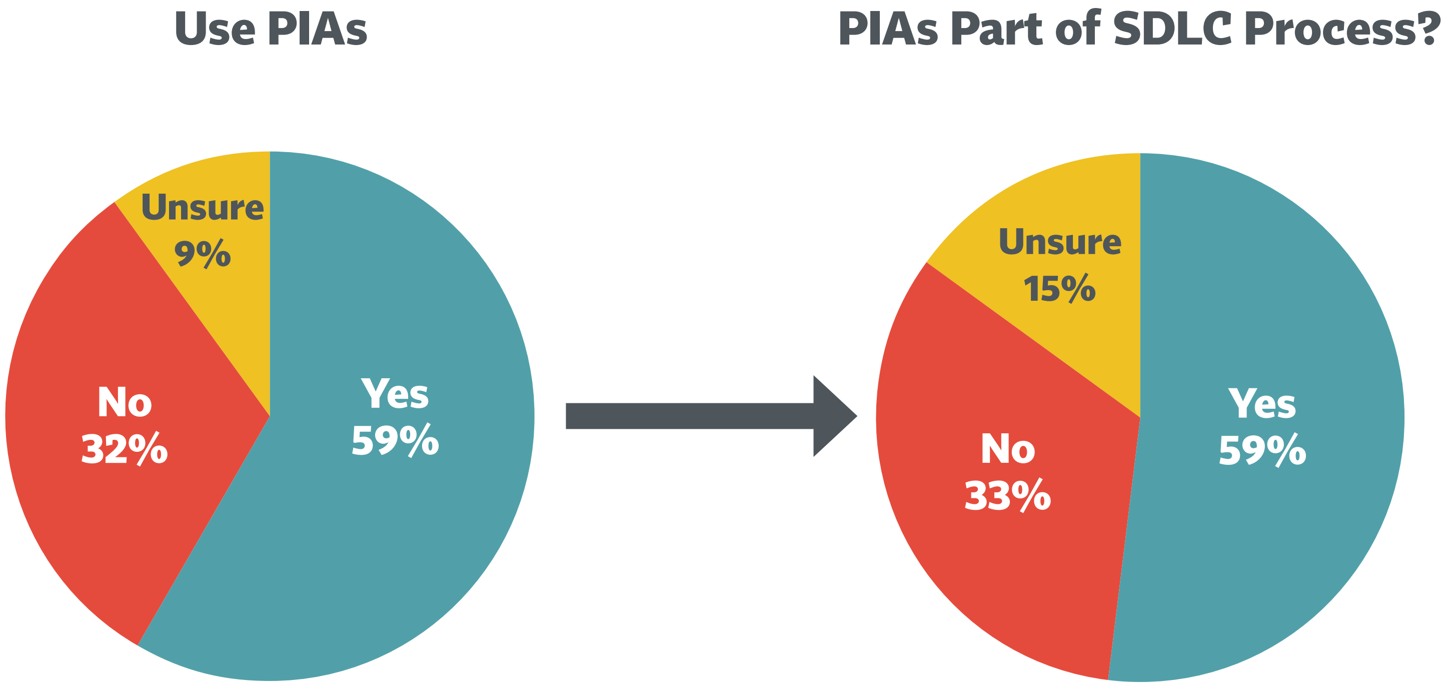




H14: Your company's GRC tools are…
H15: Over the course of the next year, you expect privacy-related activities to be integrated into a GRC tool …

# 6 in 10 professionals use Privacy Impact Assessments at their firm

- Of those who use PIAs, about half say they're part of their company's Systems Development Lifecyle process (with 15% not sure)



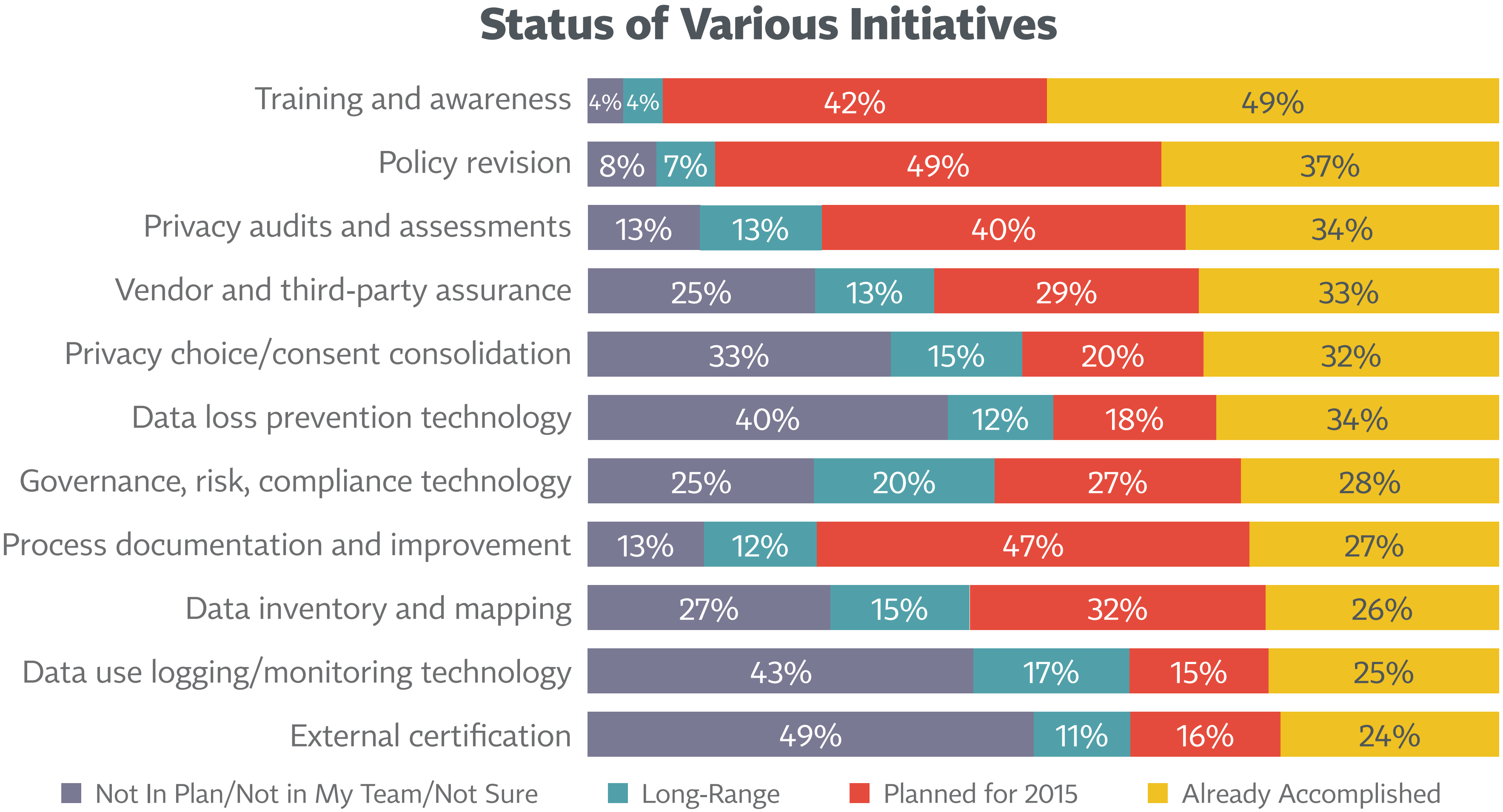
H16: Does your company use Privacy Impact Assessments (PIAs)?
H17: Are PIAs part of your company's Systems Development Life Cycle (SDLC) process?

4

# The Future and Speculation

# Training/awareness, policy revision, and privacy audits are the projects most likely to be already accomplished

- Those, along with process documentation and improvement, are also the most likely to be on the docket for 2015

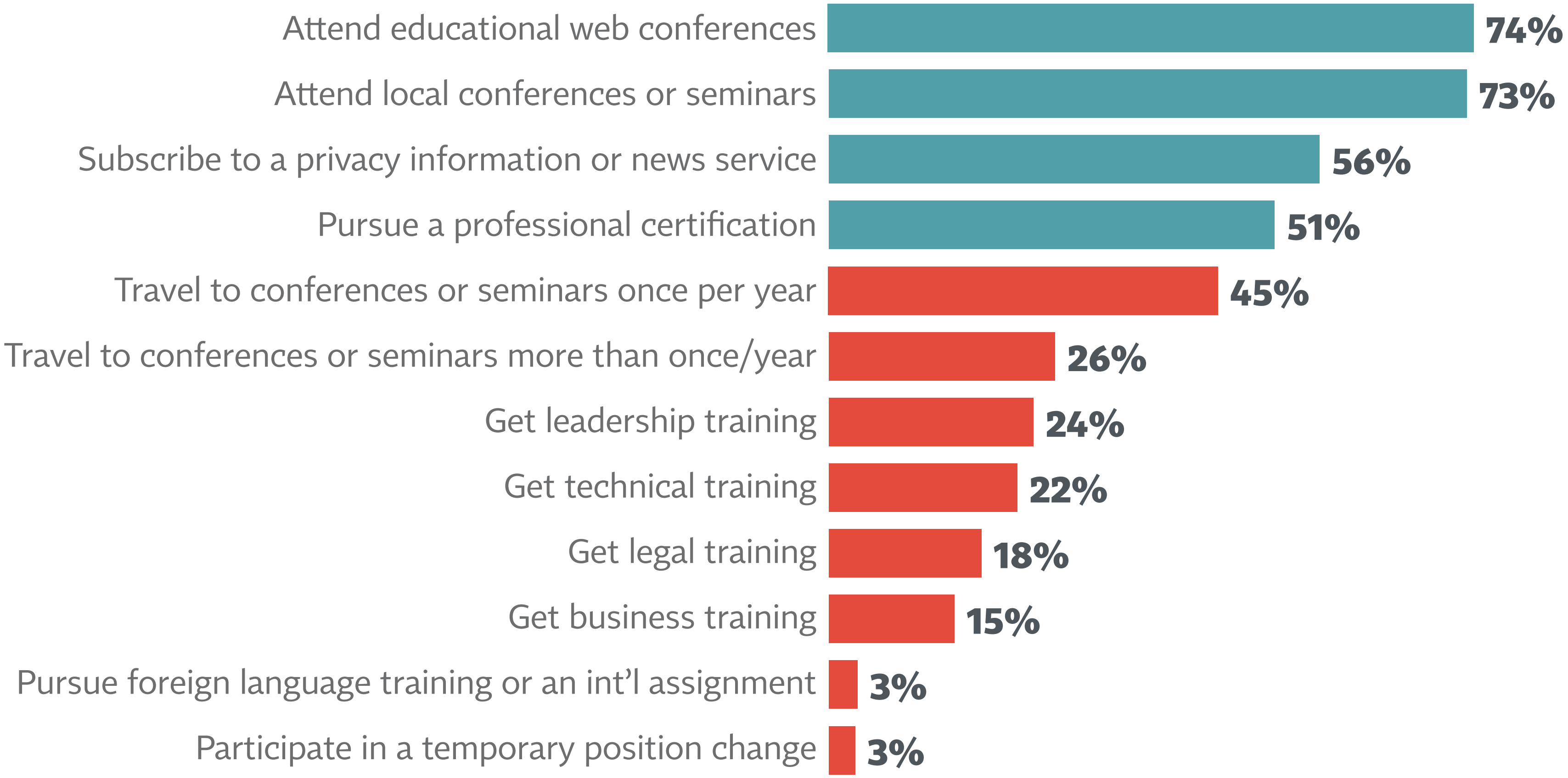


E7: For each of the following possible projects, please tell us whether the project is …

# By far the activities most likely to be planned for the next year are attending web and local conferences

- Also notable: 51% say they plan to pursue certification

## Activities Planned for Next 12 Months



D6: And which learning and growth activities are you authorized and planning to do over the next 12 months?

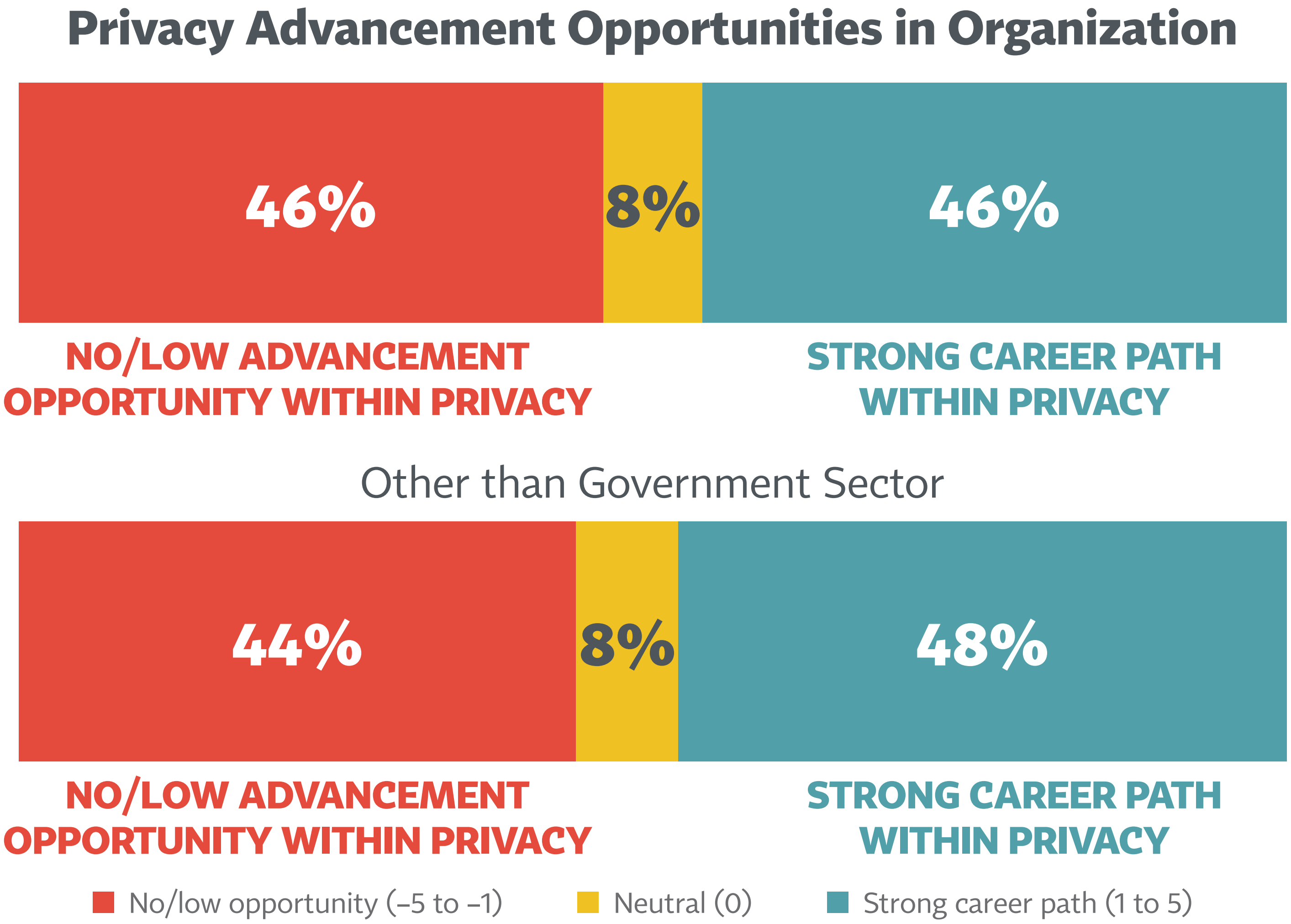
4

# The Future and Speculation

- The Future and Speculation: The Future
- **The Future and Speculation: Thoughts About the Profession**

# Professionals are evenly split in their assessment of career path opportunities in their current group

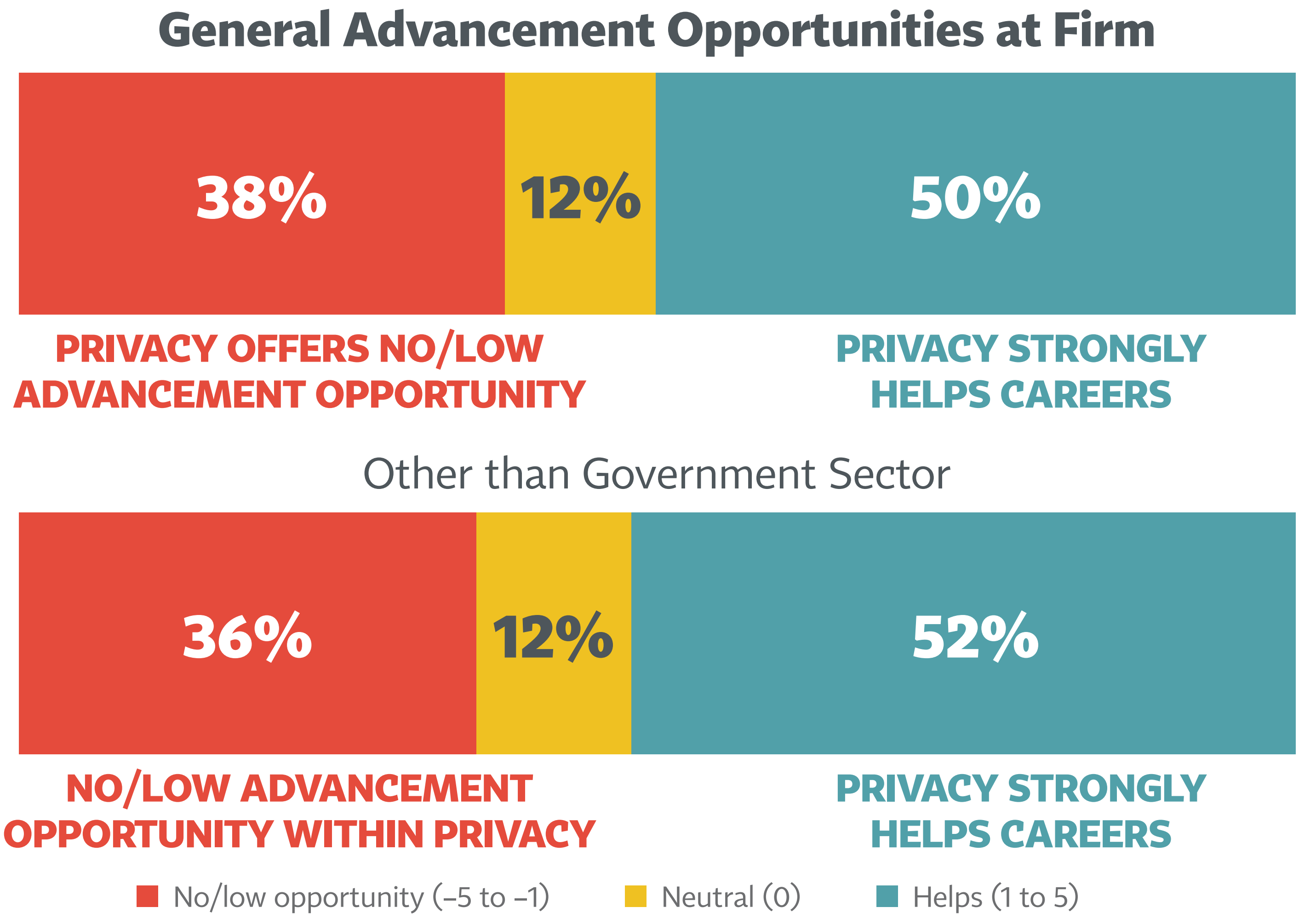
- 46% give a generally positive assessment; another 46% give a relatively negative assessment



E9: Please use the slider below to indicate the extent to which you view privacy as a career track at your organization.

## Respondents are somewhat more positive when asked how privacy helps boost advancement in the firm

- In other words, professionals are a bit more likely to feel privacy experience will help someone advance elsewhere in the company than in their own department

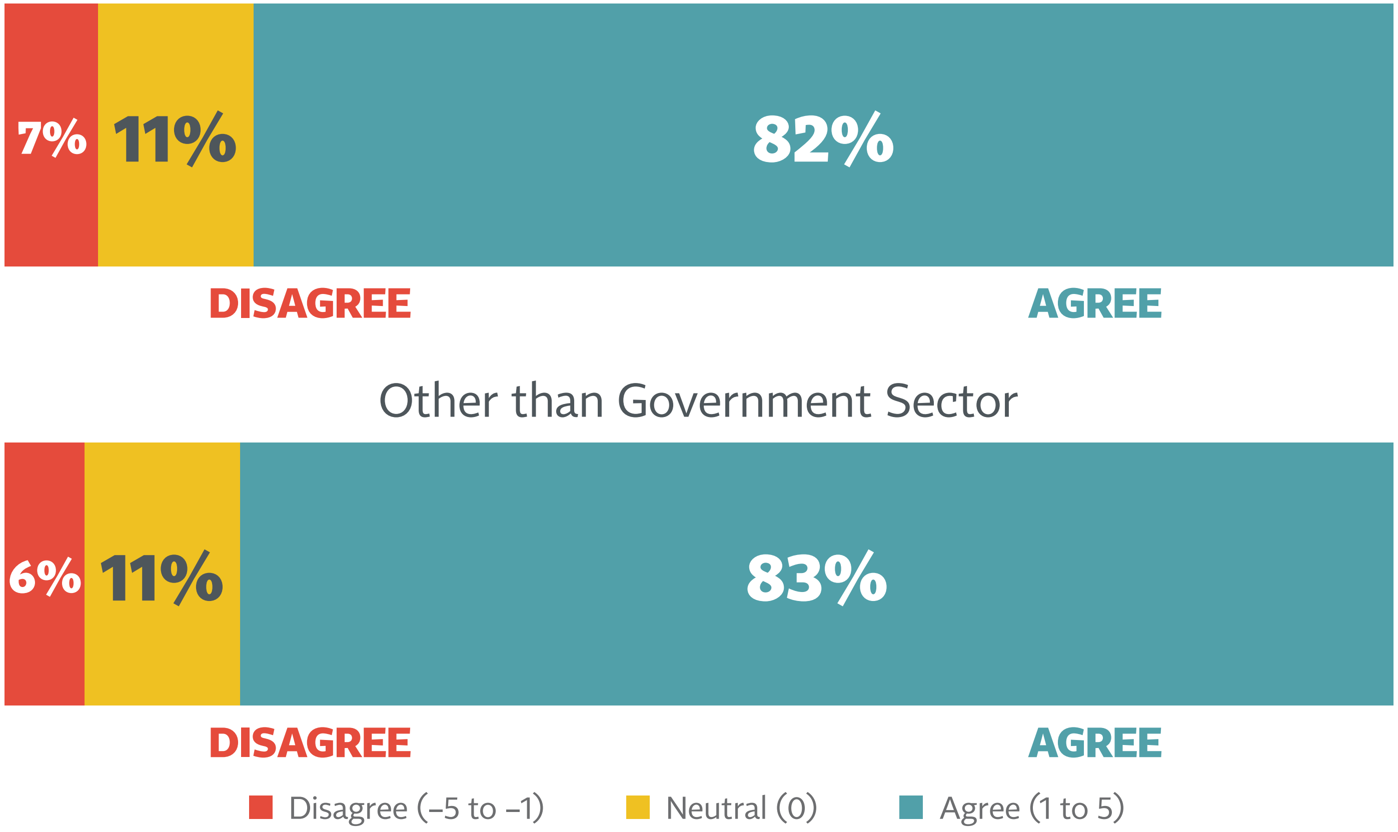


E10: Again, please use the slider below to indicate the extent to which privacy roles can advance careers at your company in general (that is, not necessarily within the privacy program).

# Much more unequivocal: the positive impact that privacy experience has on one's career in general

- More than 8 in 10 agree that strong privacy experience helps open doors in the marketplace overall

## Privacy Helps Open Career Doors?



E11: Please indicate the degree to which you agree or disagree with the following statement:
Doing well in privacy will open doors for better and better job opportunities in the marketplace.

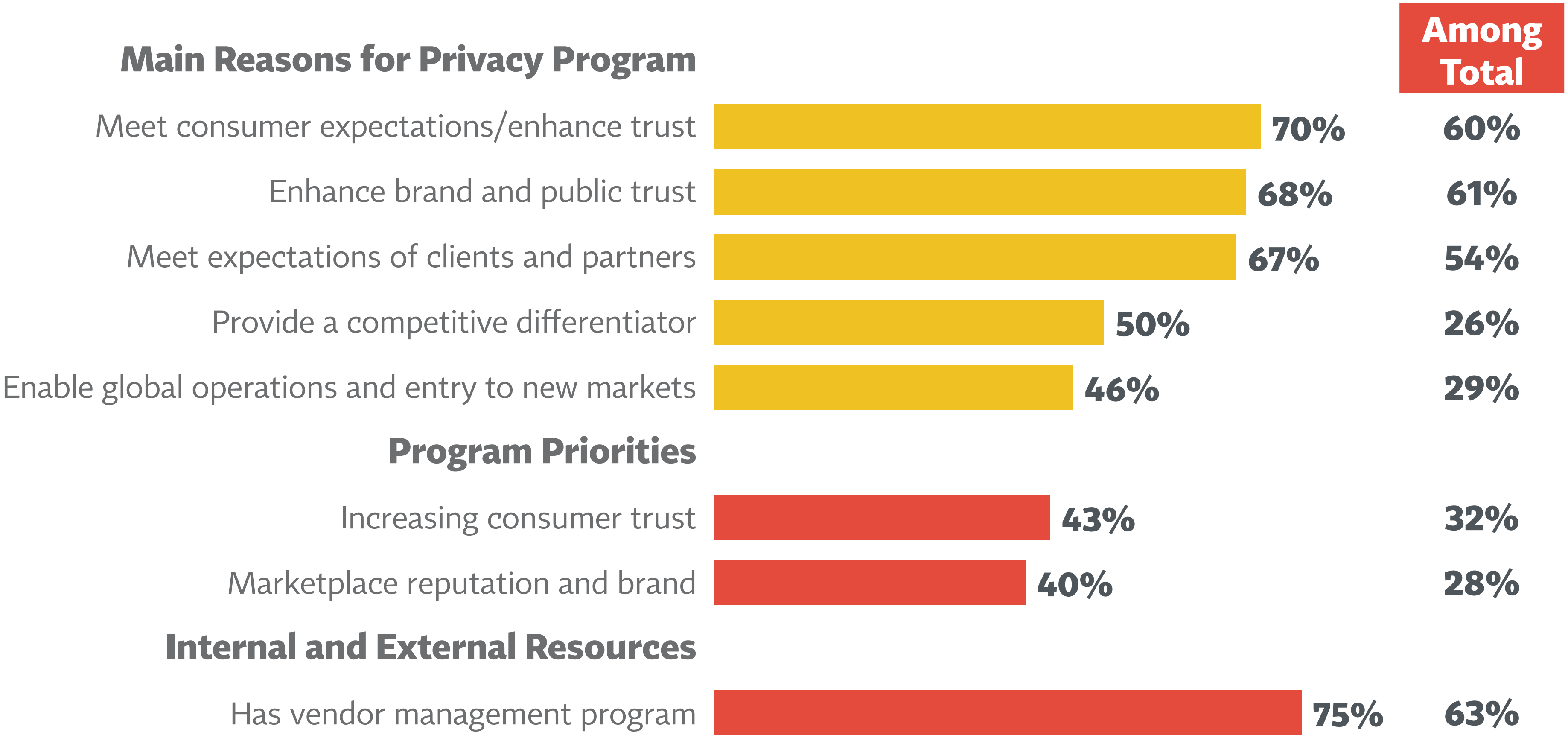
5

# Key Segment Differences

- **Key Segment Differences**
- Key Segment Differences: Region
- Key Segment Differences: Company Size
- Key Segment Differences: Maturity
- Key Segment Differences: Industry

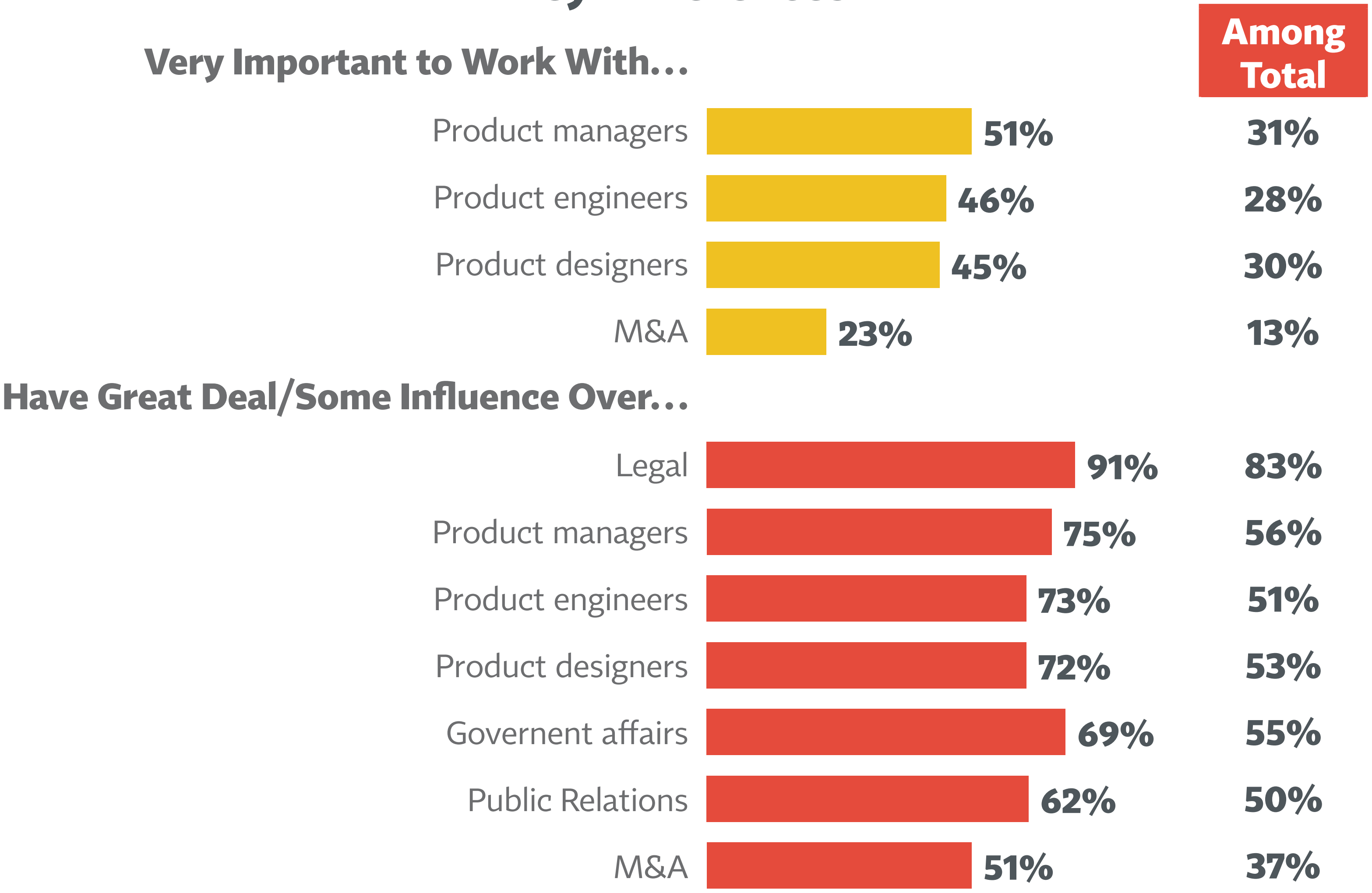
# Professionals in software and service firms are more likely to say privacy is about brand and consumer trust

## Key Differences

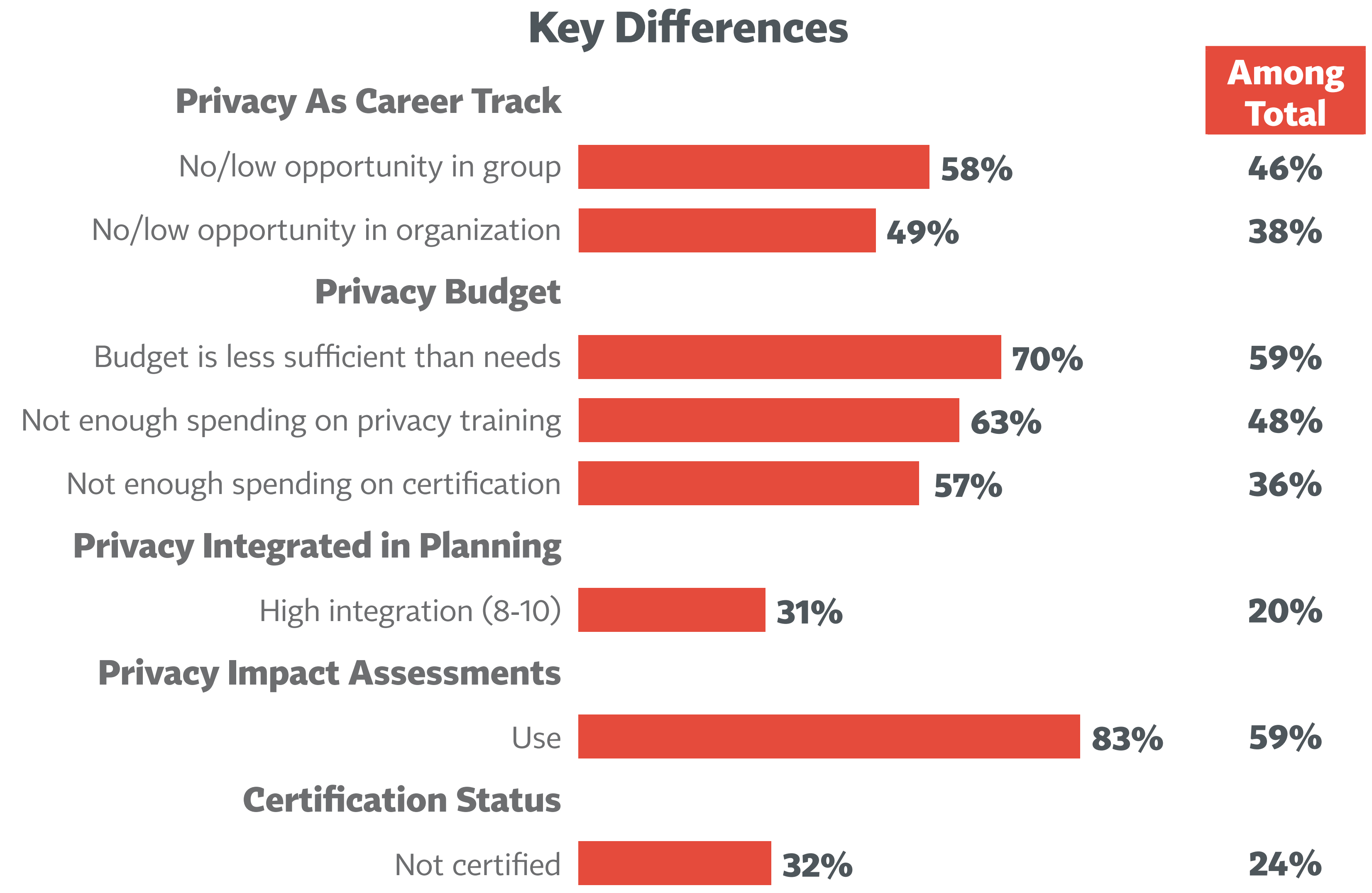


# Software/service professionals are also more likely than average to have influence over *product* departments

## Key Differences



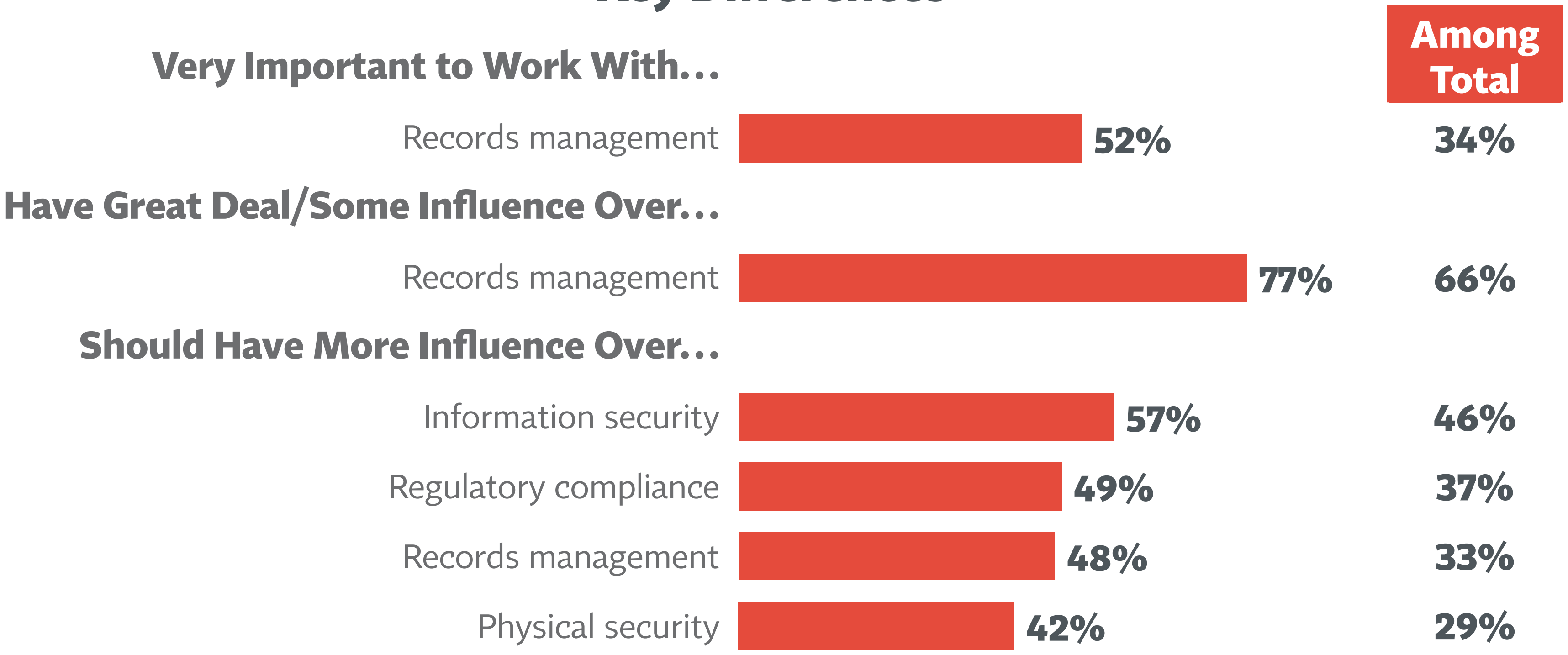
# Professionals in government tell a tale of low career opportunities and insufficient budgets



# Government professionals have more influence than average over records management groups

- However, they're much more likely than average to want greater influence over IS and compliance than they currently have

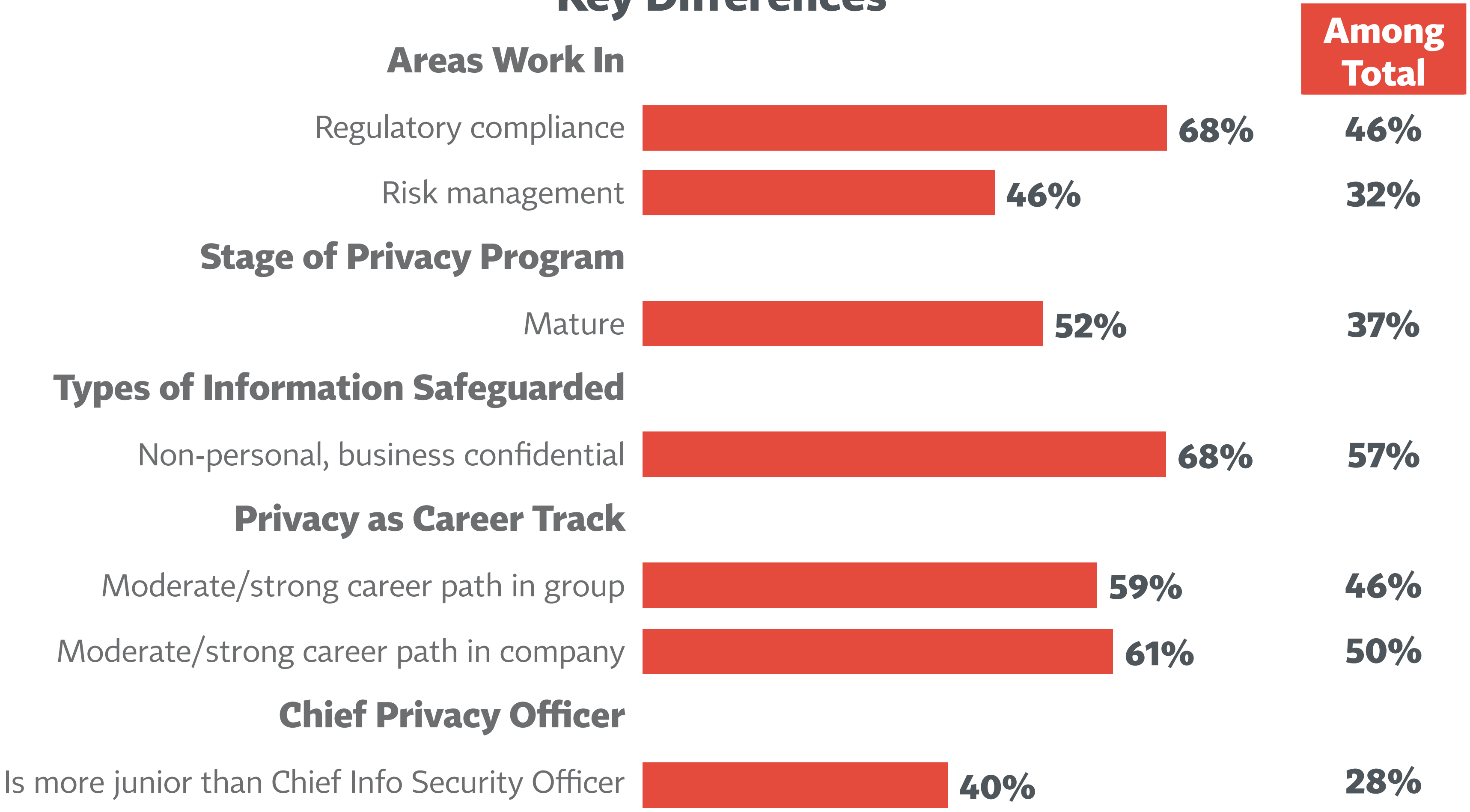
## Key Differences



# Banking privacy professionals are more likely than average to see strong career opportunities for privacy

- They're also more likely to say their privacy stage is mature, even though they're also more likely to cite chief privacy officers whose level is lower than chief IS officers

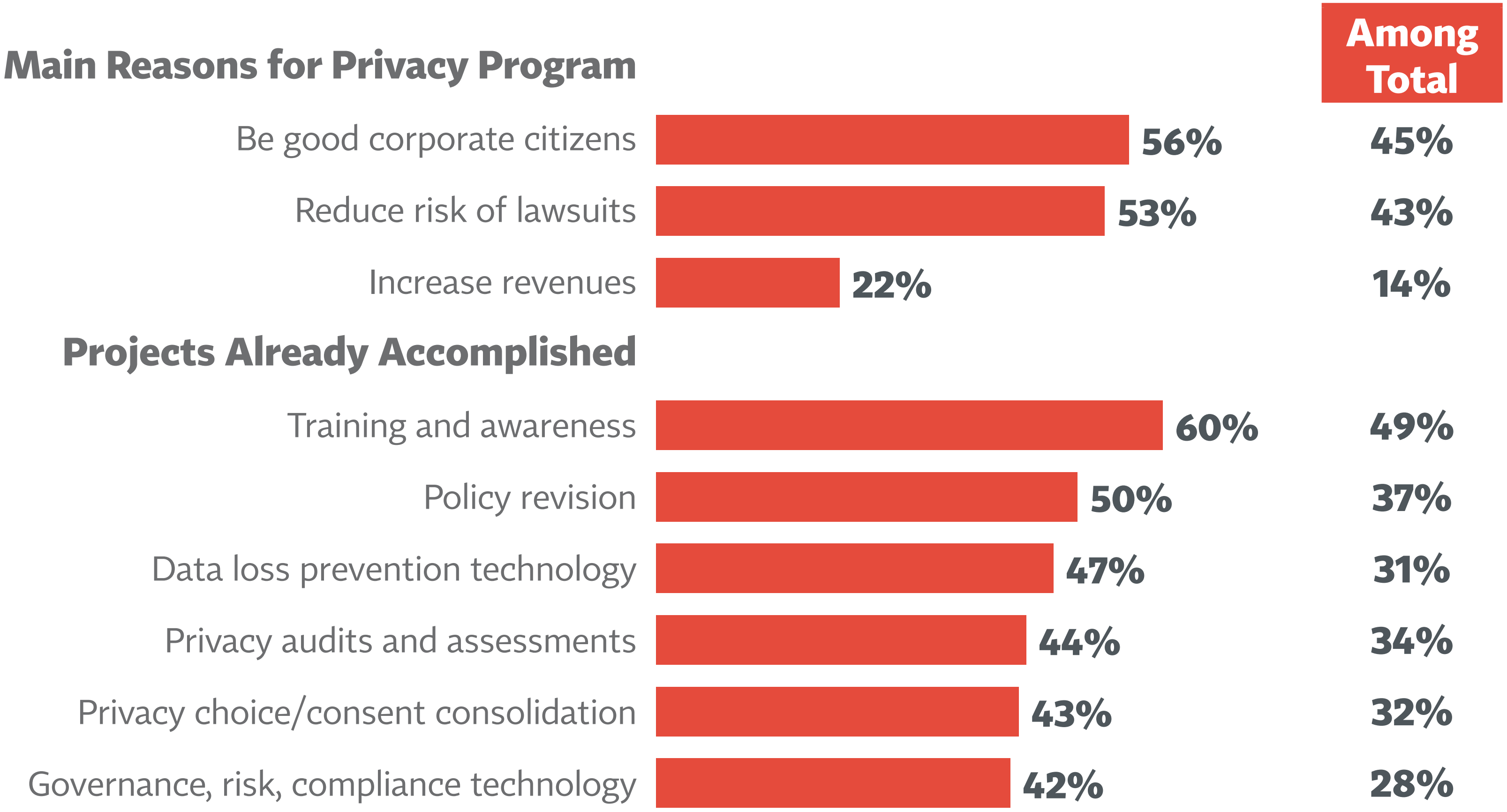
## Key Differences



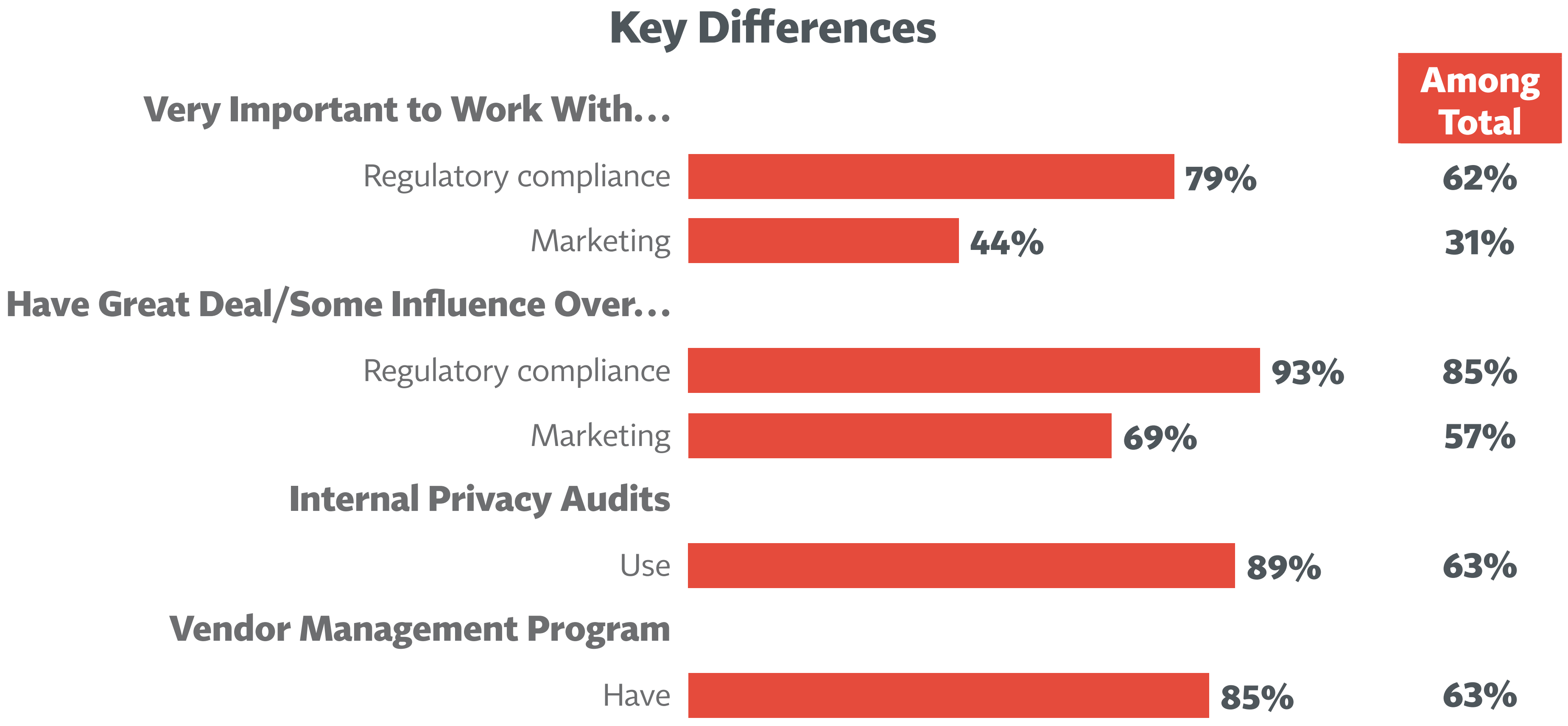
# Privacy professionals in banking are more likely to cite two main reasons for having a privacy program…

- …to be good corporate citizens AND to reduce the risk of lawsuits

## Key Differences



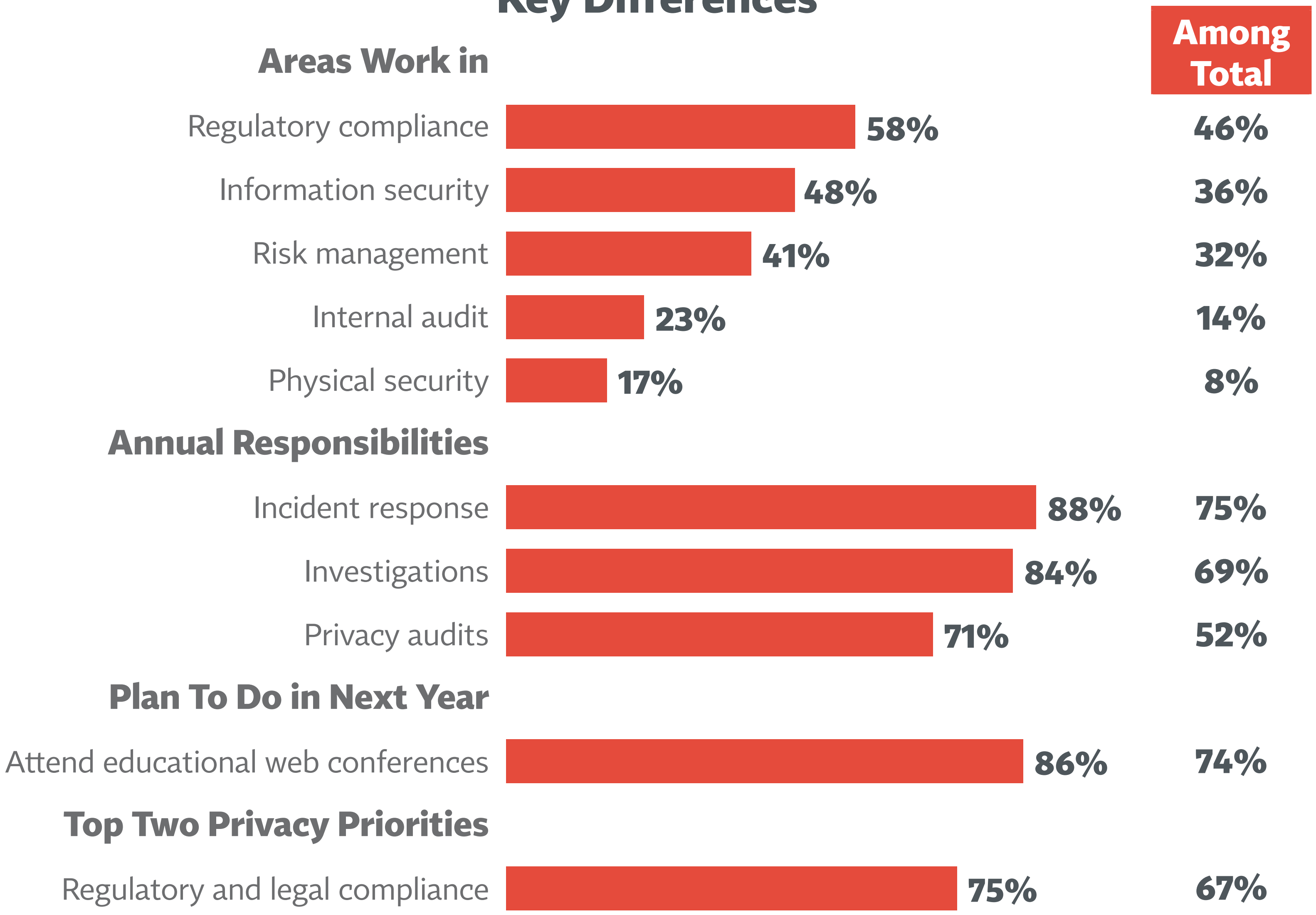
# Banking professionals have greater than average influence over compliance and marketing



# Healthcare professionals are more likely to work in compliance and information security

- They're also more likely to be involved in incident response, investigations and audits.

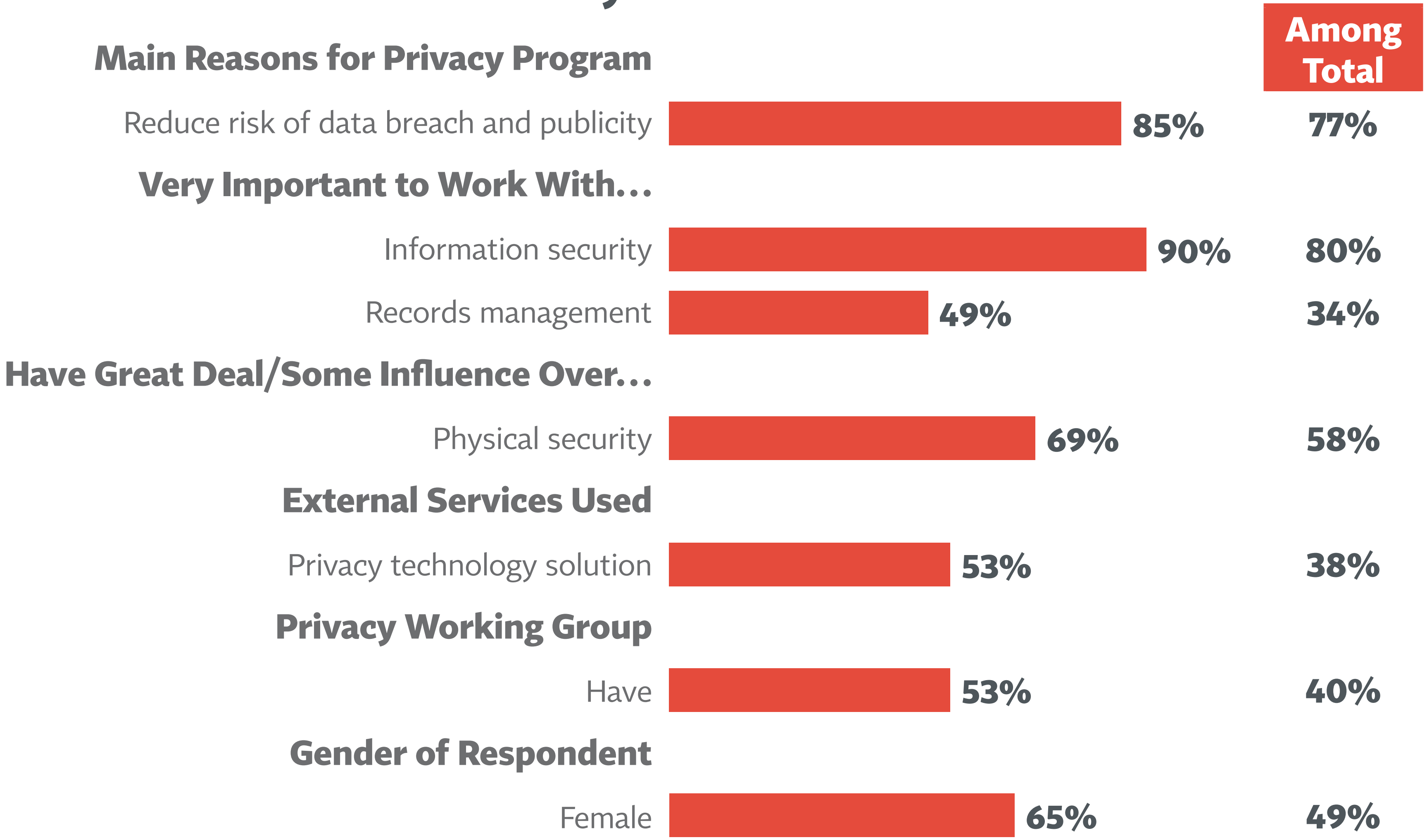
## Key Differences



# Healthcare pros are more apt to say their privacy program was created to reduce data breach risk

- Indeed, information and physical security is a common theme throughout for these participants

Key Differences



# In looking at the Privacy Leader/CPO vs. CISO positions:

- Early stage organizations are **more likely to not have a CISO** (18%), compared to Middle (9%) and Mature (5%).
- This is also the case as **employee size exceeds 2500**: <2500 (18%), 2500-24999 (7%), 25000+ (5%)
- Having the CISO be an equivalent position to the CPO is **more common as maturity increases** - Early (25%), Mid (40%), Mature (48%)
- This is also the case as **employee size exceeds 2500**: <2500 (26%), 2500-24999 (44%), 25000+ (47%)
- The CPO and CISO are **more likely to be the same person** for smaller companies than for larger ones: <2500 employees (18%), 2500-24999 (6%), 25000+ (9%)

**As firms mature, the CPO is more likely to be equivalent to the CISO**

# In looking at when representatives of the privacy function get involved:

- For ongoing projects Mature stage organizations are **more likely to be involved at the outset** (39%), compared to Middle (30%) and Early (23%)
- Similarly, Mature orgs are **more likely to be involved on an ongoing basis** (56%), compared to Middle (38%), and Early (31%)
- For new projects Mature organizations are **more likely to become involved at the development phase** (74%), compared to Middle (56%), and Early (41%)
- Early stage organizations are **more likely to be brought in only when needed** (41%), compared to Middle (30%) and Mature (17%)

**As firms mature, privacy by design starts to become more commonpace**

# 5 Key Segment Differences

- Key Segment Differences
- **Key Segment Differences: Region***
- Key Segment Differences: Company Size
- Key Segment Differences: Maturity
- Key Segment Differences: Industry

*** The European respondents to the survey tend to work for multinational companies based in the U.S. This means that the sample does not represent the European market at large but rather the specific subset of large corporations operating in Europe.**

# For privacy structure, the U.S. and EU are similar, with one exception…

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Department Structure** | | | |
| Vertical rungs (mean) | 3 | 3 | 3 |
| Horizontal rungs (mean) | 4 | 3 | 4 |
| Vertical rungs above privacy lead (mean) | 3 | 3 | 3 |
| **Privacy leader responsibilities are 100% privacy** | **44%** | **38%** | **60%** |
| **Reporting Structure** | | | |
| All/most report to same person | 73% | 72% | 71% |
| Most report to different positions | 27% | 28% | 29% |
| **Location of Department** | | | |
| At headquarters only | 43% | 43% | 16% |
| Mostly at headquarters with some members disbursed | 30% | 33% | 35% |
| Mostly spread across regional offices with some at headquarters | 23% | 21% | 42% |
| Across our regional offices with none at headquarters | 4% | 3% | 6% |

**6 out of 10 in the EU focus on privacy exclusively**

# The U.S. and EU are similar in satisfaction with department and with type of focus

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Department Housing Privacy** | | | |
| Right place | 66% | 67% | 62% |
| **Compliance- Versus Risk-Based** | | | |
| Compliance-based | 41% | 41% | 36% |
| Risk-based | 47% | 48% | 48% |
| **Sector** | | | |
| Private sector in-house | 60% | 64% | 63% |
| Internal (including private sector) | 79% | 80% | 75% |
| External | 16% | 15% | 23% |

# U.S. firms are more likely than EU firms to be either in the Early or Mature stage of privacy

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Maturity stage** | | | |
| Early | 19% | 21% | 15% |
| **Middle** | **44%** | **43%** | **56%** |
| Mature | 37% | 37% | 29% |
| Number of years with privacy program (mean) | 7 | 7 | 7 |
| **Percent in Top Work Areas (mean)** | | | |
| Advising and consulting the company on privacy | 15% | 15% | 18% |
| Developing and implementing privacy policies and guidance | 11% | 11% | 11% |
| Performing privacy risk assessments and data inventories | 9% | 9% | 9% |
| Activities not related to privacy | 9% | 8% | 7% |
| Analyzing privacy regulations | 8% | 9% | 8% |
| Monitoring and measuring privacy compliance and enforcement | 8% | 8% | 7% |

**EU firms tend to cluster around the mid-maturity stage**

# Privacy practices in U.S. firms are more likely to have a certified decision-maker and a larger practice overall

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Certifications** | | | |
| **Have a CIP* certification** | **62%** | **66%** | **56%** |
| No certification | 24% | 22% | 23% |
| **Staffing** | | | |
| **Mean number of employees dedicated to privacy** | **12** | **14** | **9** |
| Expect full-time dedicated staff to increase | 31% | 34% | 34% |
| **Budget** | | | |
| **Median budget for privacy** | **$277,025** | **$500,000** | **$225,900** |
| Expect budget will increase | 31% | 34% | 32% |
| Less than sufficient to meet privacy needs | 59% | 57% | 65% |
| Proportion of privacy budget allocated to salary and travel | 51% | 48% | 54% |
| Proportion of privacy budget allocated to professional development | 9% | 9% | 9% |

**U.S. firms have more privacy employees on average**

**Privacy budgets are nearly twice as high in the U.S.**

# Reasons for having a privacy program are comparable between U.S. and EU firms

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Main Reasons for Privacy Program** | | | |
| To meet regulatory compliance obligations | 93% | 93% | 90% |
| To reduce risk of data breach notification/publicized data breaches | 77% | 77% | 73% |
| To enhance the company's brand and public trust | 61% | 59% | 64% |
| To meet consumer expectations and enhance trust | 60% | 60% | 59% |
| To meet the expectations of business clients and partners | 54% | 55% | 53% |
| To be good corporate citizens | 45% | 47% | 32% |
| To reduce the risk of employee and consumer lawsuits | 43% | 45% | 29% |
| To enable global operations and entry into new markets | 29% | 32% | 32% |
| To provide a competitive differentiator | 26% | 27% | 30% |
| To increase the value and quality of data | 23% | 24% | 18% |
| To increase revenues from cross-selling and direct marketing | 14% | 14% | 13% |
| To reduce the cost of storing data | 8% | 8% | 9% |

# However, when asked to rank their top two reasons for having a privacy program, one difference emerges

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Ranked in Top Two of Privacy Priorities** | | | |
| Regulatory and legal compliance | 67% | 66% | 63% |
| Safeguarding data against attacks and threats | 44% | 46% | 38% |
| **Increasing consumer trust** | **32%** | **30%** | **48%** |
| Marketplace reputation and brand | 28% | 27% | 33% |
| Ethical decision-making concerning use of data | 18% | 18% | 17% |
| Ensuring business partner compliance (including by service providers, outsourcing vendors) | 17% | 17% | 20% |
| Maintaining or enhancing the value of information assets | 10% | 10% | 10% |
| Increasing employee trust | 9% | 8% | 13% |

**Increasing consumer trust is a much higher priority in the EU**

# U.S. and EU firms differ on the types of resources and privacy tools they use

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Internal and External Resources** | | | |
| Have worked with privacy attorney in past year | 66% | 70% | 72% |
| **Uses internal audit for privacy audits** | **63%** | **63%** | **72%** |
| Have a Privacy Working Group | 40% | 42% | 46% |
| **Have Vendor Management Program** | **63%** | **67%** | **63%** |
| **Use GRC tools** | **42%** | **47%** | **36%** |
| Have centralized Contract Management System | 35% | 34% | 37% |
| **Use Privacy Impact Assessments (PIAs)** | **59%** | **51%** | **70%** |
| **Involved in creating privacy program** | **57%** | **56%** | **60%** |

**Internal audit and PIAs are more commonly used in the EU**

**But U.S. firms are more likely to use Vendor Management and GRC tools**

# A broad range of interaction exists between privacy and other functions in the EU

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Interact With on a Regular Basis ...** | | | |
| Information Security | 83% | 84% | 85% |
| Legal | 79% | 82% | 85% |
| Information Technology | 72% | 73% | 67% |
| **Regulatory Compliance** | **64%** | **63%** | **74%** |
| **Human Resources** | **56%** | **54%** | **63%** |
| **Internal Audit** | **45%** | **44%** | **52%** |
| **Marketing** | **42%** | **43%** | **52%** |
| **Product Managers** | **40%** | **43%** | **48%** |
| Records Management | 39% | 37% | 22% |

**EU decision-makers are a bit more likely to interact with Regulatory Compliance, Internal Audit, HR and the product/ marketing groups**

# U.S. and EU organizations cite similar levels of influence over other departments

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Have Great Deal or Some Influence Over (top functions) . . .** | | | |
| Information Security | 87% | 86% | 87% |
| Regulatory Compliance | 85% | 85% | 87% |
| Legal | 83% | 85% | 87% |
| Information Technology | 81% | 82% | 73% |
| Human Resources | 73% | 72% | 75% |
| Corporate Ethics | 70% | 71% | 69% |
| Records Management | 66% | 65% | 55% |
| Internal Audit | 65% | 63% | 72% |

# EU privacy decision-makers are much more likely to say they want more influence over other functions

## Key Differences by Region

| SHOULD Have Great Deal or Some More Influence Over (top functions) … | ALL | U.S. | EU |
|---|---|---|---|
| Information Technology | 46% | 43% | 59% |
| Information Security | 46% | 44% | 52% |
| Corporate Ethics | 41% | 38% | 47% |
| Human Resources | 41% | 39% | 59% |
| Product Designers | 38% | 38% | 47% |
| Regulatory Compliance | 37% | 35% | 39% |
| Product Managers | 37% | 37% | 44% |
| Product Engineers | 36% | 37% | 45% |

**Privacy professionals in the EU would like to have more say in the workings of a range of departments**

# For privacy initiatives accomplished, the EU beats the U.S. in many areas

## Key Differences by Region

| | ALL | U.S. | EU |
|---|---|---|---|
| **Projects Accomplished** | | | |
| **Training and awareness** | **49%** | **48%** | **54%** |
| **Policy revision** | **37%** | **37%** | **46%** |
| **Privacy audits and assessments** | **34%** | **33%** | **39%** |
| Vendor and third-party assurance | 33% | 34% | 34% |
| **Privacy choice and consent consolidation** | **32%** | **29%** | **41%** |
| **Data loss prevention technology** | **31%** | **34%** | **26%** |
| Governance, risk and compliance technology | 28% | 29% | 29% |
| **Process documentation and improvement** | **27%** | **26%** | **32%** |
| Data inventorying and mapping | 26% | 27% | 25% |
| Data use logging and monitoring technology | 25% | 25% | 25% |
| External certification | 24% | 25% | 20% |

**Those in the EU are also more likely than those in the U.S. to have met a range of initiatives; the one exception is a greater focus on data loss prevention in the U.S.**

5

# Key Segment Differences

- Key Segment Differences
- Key Segment Differences: Region
- **Key Segment Differences: Company Size**
- Key Segment Differences: Maturity
- Key Segment Differences: Industry

# Larger companies have departments that are larger both vertically and horizontally

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Department Structure** | | | | |
| Vertical rungs (mean) | 3 | 2 | 2 | 3 |
| Horizontal rungs (mean) | 4 | 2 | 4 | 5 |
| Vertical rungs above privacy lead (mean) | 3 | 2 | 3 | 3 |
| Privacy leader responsibilities are 100% privacy | 44% | 13% | 37% | 51% |
| **Reporting Structure** | | | | |
| All/most report to same person | 73% | 76% | 79% | 66% |
| Most report to different positions | 27% | 24% | 21% | 34% |
| **Location of Department** | | | | |
| At headquarters only | 43% | 73% | 47% | 19% |
| Mostly at headquarters with some members disbursed | 30% | 14% | 31% | 40% |
| Mostly spread across regional offices with some at headquarters | 23% | 9% | 18% | 38% |
| Across our regional offices with none at headquarters | 4% | 3% | 4% | 3% |

**The largest firms have more of a privacy hierarchy and more decentralized privacy organizations; they're also more likely to have a privacy leader dedicated entirely to privacy tasks**

# Smaller firms tend to be more compliance-focused and are more likely to rely on an external privacy lead

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Department Housing Privacy** | | | | |
| Right place | 66% | 70% | 65% | 65% |
| **Compliance- Versus Risk-Based** | | | | |
| Compliance-based | 41% | 48% | 43% | 35% |
| Risk-based | 47% | 42% | 45% | 53% |
| **Sector** | | | | |
| Private sector in-house | 60% | 42% | 65% | 71% |
| Internal (including private sector) | 79% | 62% | 89% | 85% |
| External | 16% | 32% | 8% | 10% |

**The larger the firm, the more likely it is to be primarily risk-focused**

# Larger companies tend to be further along the maturity spectrum

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Maturity Stage** | | | | |
| **Early** | **19%** | **31%** | **18%** | **12%** |
| **Middle** | **44%** | **44%** | **49%** | **40%** |
| **Mature** | **37%** | **25%** | **33%** | **48%** |
| **Number of years with privacy program (mean)** | **7** | **6** | **7** | **9** |
| **Percent in Top Work Areas (mean)** | | | | |
| Advising and consulting the company on privacy | 15% | 13% | 16% | 16% |
| Developing and implementing privacy policies and guidance | 11% | 11% | 10% | 11% |
| Performing privacy risk assessments and data inventories | 9% | 7% | 9% | 10% |
| **Activities not related to privacy** | **9%** | **13%** | **7%** | **7%** |
| Analyzing privacy regulations | 8% | 9% | 8% | 8% |
| Monitoring and measuring privacy compliance and enforcement | 8% | 9% | 9% | 7% |

**It comes as no surprise that the largest firms have the most mature privacy practice**

**In line with the earlier finding on dedication to privacy, decision-makers in smaller firms spend more time on non-privacy tasks**

# Larger firms have more—and more professionally certified—privacy resources at their disposal

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Certifications** | | | | |
| Have a CIP* certification | 62% | 54% | 65% | 67% |
| No certification | 24% | 30% | 23% | 18% |
| **Staffing** | | | | |
| Mean number of employees dedicated to privacy | 12 | 2 | 5 | 24 |
| Expect full-time dedicated staff to increase | 31% | 17% | 31% | 41% |
| **Budget** | | | | |
| Median budget for privacy | $277,025 | $75,000 | $250,000 | $1,000,000 |
| Expect budget will increase | 31% | 29% | 32% | 33% |
| Less than sufficient to meet privacy needs | 59% | 57% | 65% | 55% |
| Proportion of privacy budget allocated to salary and travel | 51% | 45% | 51% | 54% |
| Proportion of privacy budget allocated to professional development | 9% | 12% | 8% | 8% |

**Privacy professionals in large firms are more likely to have CIP* certification, in small firms, 1 in 3 are not certified at all**

**Large firms not only have the biggest privacy budget by far, but they're also most likely to expect a budget increase**

**Interestingly, mid-sized firms are the most likely to feel their privacy budgets are insufficient**

# Branding and marketing are more important components of privacy for the largest firms

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Main Reasons for Privacy Program** | | | | |
| To meet regulatory compliance obligations | 93% | 91% | 92% | 94% |
| To reduce risk of data breach notification/publicized data breaches | 77% | 75% | 80% | 75% |
| **To enhance the company's brand and public trust** | **61%** | **56%** | **57%** | **68%** |
| To meet consumer expectations and enhance trust | 60% | 61% | 57% | 63% |
| **To meet the expectations of business clients and partners** | **54%** | **53%** | **53%** | **55%** |
| **To be good corporate citizens** | **45%** | **44%** | **36%** | **53%** |
| **To reduce the risk of employee and consumer lawsuits** | **43%** | **36%** | **41%** | **49%** |
| **To enable global operations and entry into new markets** | **29%** | **18%** | **26%** | **39%** |
| **To provide a competitive differentiator** | **26%** | **24%** | **20%** | **34%** |
| **To increase the value and quality of data** | **23%** | **24%** | **18%** | **26%** |
| To increase revenues from cross-selling and direct marketing | 14% | 11% | 11% | 18% |
| To reduce the cost of storing data | 8% | 8% | 8% | 9% |

**The largest firms have the broadest range of privacy "reasons for being"—including using privacy to enhance public trust**

# However, “top two” priorities for privacy are comparable across firm sizes

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Ranked in Top Two of Privacy Priorities** | | | | |
| Regulatory and legal compliance | 67% | 67% | 68% | 66% |
| **Safeguarding data against attacks and threats** | **44%** | **51%** | **40%** | **44%** |
| Increasing consumer trust | 32% | 30% | 31% | 35% |
| Marketplace reputation and brand | 28% | 27% | 28% | 29% |
| Ethical decision-making concerning use of data | 18% | 19% | 15% | 21% |
| Ensuring business partner compliance (including by service providers, outsourcing vendors) | 17% | 14% | 16% | 19% |
| Maintaining or enhancing the value of information assets | 10% | 12% | 8% | 12% |
| **Increasing employee trust** | **9%** | **7%** | **7%** | **12%** |

**Small firms place a relatively higher priority on safeguarding themselves against data threats**

# The largest firms, not surprisingly, have a range of privacy programs and tools in place

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Internal and External Resources** | | | | |
| Have worked with privacy attorney in past year | 66% | 56% | 65% | 74% |
| Uses internal audit for privacy audits | 63% | 54% | 58% | 73% |
| Have a Privacy Working Group | 40% | 33% | 38% | 46% |
| Have Vendor Management Program | 63% | 48% | 66% | 71% |
| Use GRC tools | 42% | 18% | 42% | 58% |
| Have centralized Contract Management System | 35% | 34% | 40% | 31% |
| Use Privacy Impact Assessments (PIAs) | 59% | 52% | 58% | 64% |
| **Involved in creating privacy program** | 57% | 70% | 62% | 45% |

**With the exception of Contract Management Systems, the largest firms are much more likely than others to engage in the full range of initiatives tested**

**The smaller the firm, the more likely it is that the privacy decision-maker had a role in developing the privacy program**

# Large firms are especially likely to work close with Legal, Compliance and Marketing

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Interact With on a Regular Basis …** | | | | |
| Information Security | 83% | 77% | 86% | 85% |
| **Legal** | **79%** | **65%** | **83%** | **86%** |
| Information Technology | 72% | 74% | 71% | 71% |
| **Regulatory Compliance** | **64%** | **53%** | **66%** | **71%** |
| Human Resources | 56% | 54% | 52% | 60% |
| **Internal Audit** | **45%** | **33%** | **45%** | **53%** |
| **Marketing** | **42%** | **36%** | **41%** | **47%** |
| Product Managers | 40% | 37% | 41% | 42% |
| Records Management | 39% | 39% | 40% | 39% |

**Those in the largest firms are more likely to interact regularly with Legal and Regulatory Compliance—along with Internal Audit and Marketing**

# Influence over other departments doesn't vary much by size of firm, with one exception

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Have Great Deal or Some Influence Over (top functions) …** | | | | |
| Information Security | 87% | 85% | 88% | 86% |
| Regulatory Compliance | 85% | 84% | 83% | 87% |
| Legal | 83% | 79% | 83% | 86% |
| Information Technology | 81% | 80% | 82% | 82% |
| Human Resources | 73% | 71% | 71% | 75% |
| Corporate Ethics | 70% | 70% | 67% | 73% |
| **Records Management** | **66%** | **74%** | **65%** | **61%** |
| Internal Audit | 65% | 68% | 62% | 65% |

**When it comes to influence over other functions, one difference stands out: small firms' influence over Records Management**

# We also find just one exception in functions professionals WANT more influence over

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **SHOULD Have Great Deal or Some More Influence Over (top functions) …** | | | | |
| Information Technology | 46% | 49% | 42% | 49% |
| Information Security | 46% | 51% | 41% | 46% |
| **Corporate Ethics** | **41%** | **49%** | **39%** | **37%** |
| Human Resources | 41% | 44% | 38% | 42% |
| Product Designers | 38% | 37% | 35% | 43% |
| Regulatory Compliance | 37% | 42% | 32% | 38% |
| Product Managers | 37% | 35% | 37% | 38% |
| Product Engineers | 36% | 35% | 33% | 40% |

**And one difference stands out for the functions that privacy professionals would LIKE to have more influence over: Those in the smallest firms want more say in what Corporate Ethics does**

# Only two differences emerge in initiatives accomplished by size of firm

## Key Differences by Company Size

| | ALL | < 2500 | 2500 – 24,999 | 25,000+ |
|---|---|---|---|---|
| **Projects Accomplished** | | | | |
| Training and awareness | 49% | 49% | 48% | 51% |
| Policy revision | 37% | 34% | 36% | 40% |
| **Privacy audits and assessments** | **34%** | **30%** | **31%** | **40%** |
| Vendor and third-party assurance | 33% | 30% | 33% | 35% |
| Privacy choice and consent consolidation | 32% | 32% | 31% | 34% |
| Data loss prevention technology | 31% | 31% | 30% | 31% |
| Governance, risk and compliance technology | 28% | 24% | 28% | 32% |
| Process documentation and improvement | 27% | 25% | 27% | 29% |
| **Data inventorying and mapping** | **26%** | **24%** | **21%** | **30%** |
| Data use logging and monitoring technology | 25% | 28% | 21% | 27% |
| External certification | 24% | 25% | 23% | 24% |

**Privacy Audits and Data Inventorying are more likely to have been recently ticked off by the largest firms**

5

# Key Segment Differences

- Key Segment Differences
- Key Segment Differences: Region
- Key Segment Differences: Company Size
- **Key Segment Differences: Maturity**
- Key Segment Differences: Industry

# Mature privacy programs differ from others in both their reporting structure and physical location

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Department Structure** | | | | |
| Vertical rungs (mean) | 3 | 2 | 2 | 3 |
| Horizontal rungs (mean) | 4 | 3 | 3 | 4 |
| Vertical rungs above privacy lead (mean) | 3 | 2 | 3 | 3 |
| **Privacy leader responsibilities are 100% privacy** | **44%** | **31%** | **46%** | **50%** |
| **Reporting Structure** | | | | |
| **All/most report to same person** | **73%** | **67%** | **72%** | **78%** |
| **Most report to different positions** | **27%** | **33%** | **28%** | **22%** |
| **Location of Department** | | | | |
| **At headquarters only** | **43%** | **62%** | **42%** | **33%** |
| **Mostly at headquarters with some members disbursed** | **30%** | **16%** | **32%** | **37%** |
| **Mostly spread across regional offices with some at headquarters** | **23%** | **18%** | **22%** | **27%** |
| Across our regional offices with none at headquarters | 4% | 4% | 4% | 4% |

**Unlike large firms, firms with mature privacy programs are more likely to have centralized privacy reporting, although they're less likely to be housed at headquarters**

**Firms with mature programs are more likely to have a fully dedicated privacy lead**

# Mature programs also differ in their primary focus, with more emphasis placed on risk than compliance

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Department Housing Privacy** | | | | |
| Right place | 66% | 59% | 65% | 71% |
| **Compliance- Versus Risk-Based** | | | | |
| Compliance-based | 41% | 51% | 41% | 36% |
| Risk-based | 47% | 38% | 48% | 52% |

**Decision-makers in mature programs are happier with where their department is located—and they're more likely to be focused on risk avoidance than compliance**

# By definition, mature programs have had more time to develop their privacy practice

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Maturity Stage** | | | | |
| **Number of years with privacy program (mean)** | **7** | **2** | **7** | **11** |
| | | | | |
| **Percent in Top Work Areas (mean)** | | | | |
| Advising and consulting the company on privacy | 15% | 15% | 14% | 17% |
| Developing and implementing privacy policies and guidance | 11% | 11% | 11% | 10% |
| Performing privacy risk assessments and data inventories | 9% | 7% | 9% | 9% |
| Activities not related to privacy | 9% | 11% | 7% | 7% |
| Analyzing privacy regulations | 8% | 10% | 8% | 7% |
| Monitoring and measuring privacy compliance and enforcement | 8% | 6% | 9% | 9% |

**As one might expect, the more mature the program, the longer they've had a privacy program, in fact, early-stage programs have only been in place for two years on average**

# Mature programs differ markedly across a range of measures related to program size and expertise

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Certifications** | | | | |
| **Have a CIP* certification** | **62%** | **60%** | **59%** | **67%** |
| No certification | 24% | 22% | 26% | 18% |
| **Staffing** | | | | |
| **Mean number of employees dedicated to privacy** | **12** | **6** | **7** | **21** |
| Expect full-time dedicated staff to increase | 31% | 30% | 32% | 31% |
| **Budget** | | | | |
| **Median budget for privacy** | **$277,025** | **$197,875** | **$250,000** | **$406,000** |
| **Expect budget will increase** | **31%** | **40%** | **31%** | **27%** |
| **Less than sufficient to meet privacy needs** | **59%** | **68%** | **66%** | **46%** |
| **Proportion of privacy budget allocated to salary and travel** | **51%** | **40%** | **52%** | **55%** |
| Proportion of privacy budget allocated to professional development | 9% | 11% | 9% | 9% |

**Decision-makers in mature programs are more likely to have CIP* certification**

**Mature programs have more privacy employees and much larger privacy budgets; but firms in the early stage are the most likely to say their privacy budgets will increase**

# Supporting the brand and being good corporate citizens are stronger motivators for mature programs

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Main Reasons for Privacy Program** | | | | |
| To meet regulatory compliance obligations | 93% | 85% | 95% | 94% |
| To reduce risk of data breach notification/publicized data breaches | 77% | 66% | 79% | 80% |
| **To enhance the company's brand and public trust** | **61%** | **45%** | **58%** | **73%** |
| To meet consumer expectations and enhance trust | 60% | 46% | 59% | 69% |
| To meet the expectations of business clients and partners | 54% | 41% | 56% | 58% |
| **To be good corporate citizens** | **45%** | **32%** | **44%** | **52%** |
| To reduce the risk of employee and consumer lawsuits | 43% | 33% | 44% | 46% |
| To enable global operations and entry into new markets | 29% | 27% | 28% | 31% |
| To provide a competitive differentiator | 26% | 23% | 24% | 32% |
| To increase the value and quality of data | 23% | 17% | 23% | 26% |
| To increase revenues from cross-selling and direct marketing | 14% | 13% | 12% | 17% |
| To reduce the cost of storing data | 8% | 9% | 7% | 10% |

**The mission of firms with mature privacy programs are different in two respects: more likely to focus on enhancing brand/public trust and more focused on corporate citizenship**

# However, top priorities do not differ significantly across the privacy program maturity spectrum

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Ranked in Top Two of Privacy Priorities** | | | | |
| Regulatory and legal compliance | 67% | 68% | 66% | 67% |
| Safeguarding data against attacks and threats | 44% | 44% | 44% | 45% |
| Increasing consumer trust | 32% | 35% | 32% | 32% |
| Marketplace reputation and brand | 28% | 31% | 26% | 29% |
| Ethical decision-making concerning use of data | 18% | 18% | 15% | 22% |
| Ensuring business partner compliance (including by service providers, outsourcing vendors) | 17% | 15% | 17% | 17% |
| Maintaining or enhancing the value of information assets | 10% | 12% | 10% | 10% |
| Increasing employee trust | 9% | 9% | 8% | 10% |

# Companies with mature privacy practices rely on a range of targeted privacy tools

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Internal and External Resources** | | | | |
| Have worked with privacy attorney in past year | 66% | 56% | 69% | 68% |
| **Uses internal audit for privacy audits** | **63%** | **45%** | **60%** | **78%** |
| Have a Privacy Working Group | 40% | 30% | 42% | 43% |
| **Have Vendor Management Program** | **63%** | **40%** | **62%** | **79%** |
| **Use GRC tools** | **42%** | **28%** | **40%** | **52%** |
| **Have centralized Contract Management System** | **35%** | **35%** | **39%** | **43%** |
| **Use Privacy Impact Assessments (PIAs)** | **59%** | **36%** | **63%** | **37%** |
| **Involved in creating privacy program** | **57%** | **79%** | **60%** | **43%** |

**The more mature the privacy program, the more likely it is to be using a variety of resources and programs**

# Those in mature programs interact more with Compliance, Audit, Records Management and Product

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Interact With on a Regular Basis …** | | | | |
| Information Security | 83% | 81% | 84% | 83% |
| Legal | 79% | 75% | 80% | 81% |
| Information Technology | 72% | 73% | 75% | 68% |
| **Regulatory Compliance** | **64%** | **55%** | **60%** | **75%** |
| Human Resources | 56% | 56% | 56% | 55% |
| **Internal Audit** | **45%** | **38%** | **43%** | **50%** |
| Marketing | 42% | 35% | 41% | 46% |
| **Product Managers** | **40%** | **36%** | **39%** | **45%** |
| **Records Management** | **39%** | **34%** | **35%** | **48%** |

**Firms with mature privacy programs are more likely to have privacy and compliance working together—and are more involved with products as well**

# Mature programs are also likely to have a say in the workings of a range of other departments

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Have Great Deal or Some Influence Over (top functions) …** | | | | |
| **Information Security** | **87%** | **83%** | **86%** | **89%** |
| **Regulatory Compliance** | **85%** | **78%** | **84%** | **89%** |
| **Legal** | **83%** | **78%** | **82%** | **87%** |
| Information Technology | 81% | 81% | 79% | 84% |
| **Human Resources** | **73%** | **71%** | **69%** | **78%** |
| **Corporate Ethics** | **70%** | **60%** | **71%** | **75%** |
| Records Management | 66% | 63% | 64% | 70% |
| Internal Audit | 65% | 62% | 62% | 69% |

**Similarly, compliance is an area where mature firms have greater influence—along with legal, HR and Ethics.**

# With a fair amount of influence already, mature programs are LEAST likely to feel they need more

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **SHOULD Have Great Deal or Some More Influence Over (top functions) …** | | | | |
| Information Technology | 46% | 50% | 51% | 38% |
| Information Security | 46% | 52% | 51% | 34% |
| Corporate Ethics | 41% | 53% | 41% | 34% |
| Human Resources | 41% | 50% | 44% | 31% |
| Product Designers | 38% | 41% | 44% | 29% |
| Regulatory Compliance | 37% | 43% | 39% | 31% |
| Product Managers | 37% | 44% | 41% | 27% |
| Product Engineers | 36% | 41% | 41% | 27% |

**Early- and mid-stage programs want to have more influence over nearly every function tested**

# Companies with mature programs are more likely to have accomplished almost all top projects

## Key Differences by Maturity Phase

| | ALL | Early | Middle | Mature |
|---|---|---|---|---|
| **Projects Accomplished** | | | | |
| **Training and awareness** | **49%** | **49%** | **47%** | **64%** |
| **Policy revision** | **37%** | **27%** | **36%** | **44%** |
| **Privacy audits and assessments** | **34%** | **14%** | **32%** | **47%** |
| **Vendor and third-party assurance** | **33%** | **18%** | **32%** | **42%** |
| **Privacy choice and consent consolidation** | **32%** | **21%** | **29%** | **42%** |
| Data loss prevention technology | 31% | 23% | 31% | 34% |
| **Governance, risk and compliance technology** | **28%** | **13%** | **21%** | **46%** |
| **Process documentation and improvement** | **27%** | **12%** | **22%** | **41%** |
| **Data inventorying and mapping** | **26%** | **17%** | **22%** | **35%** |
| **Data use logging and monitoring technology** | **25%** | **17%** | **24%** | **31%** |
| **External certification** | **24%** | **17%** | **19%** | **33%** |

**Big differences emerge between mature programs and less mature programs in the full range of privacy initiatives completed**

5

# Key Segment Differences

- Key Segment Differences
- Key Segment Differences: Region
- Key Segment Differences: Company Size
- Key Segment Differences: Maturity
- **Key Segment Differences: Industry**

# Government agencies are more likely to have their privacy program at their headquarters location

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Department Structure** | | | | |
| Vertical rungs (mean) | 3 | 2 | 3 | 3 |
| Horizontal rungs (mean) | 4 | 4 | 4 | 4 |
| Vertical rungs above privacy lead (mean) | 3 | 3 | 3 | 2 |
| Privacy leader responsibilities are 100% privacy | 44% | 40% | 45% | 45% |
| **Reporting Structure** | | | | |
| All/most report to same person | 73% | 71% | 76% | 72% |
| Most report to different positions | 27% | 29% | 24% | 28% |
| **Location of Department** | | | | |
| **At headquarters only** | **43%** | **67%** | **43%** | **359%** |
| **Mostly at headquarters with some members disbursed** | **30%** | **20%** | **28%** | **34%** |
| Mostly spread across regional offices with some at headquarters | 23% | 23% | 25% | 26% |
| Across our regional offices with none at headquarters | 4% | 4% | 4% | 5% |

**Government organizations are the most likely to have privacy housed at HQ**

# Unregulated firms are especially likely to reach outside the firm for their privacy professionals

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Department Housing Privacy** | | | | |
| **Right place** | **66%** | **64%** | **70%** | **66%** |
| **Compliance- Versus Risk-Based** | | | | |
| Compliance-based | 41% | 49% | 40% | 37% |
| Risk-based | 47% | 41% | 50% | 52% |

# Distribution of time is similar for privacy professionals working in different industry sectors

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Maturity Stage** | | | | |
| Early | 19% | 19% | 16% | 20% |
| Middle | 44% | 43% | 45% | 43% |
| Mature | 37% | 38% | 39% | 36% |
| **Number of years with privacy program (mean)** | **7** | **9** | **8** | **7** |
| **Percent in Top Work Areas (mean)** | | | | |
| Advising and consulting the company on privacy | 15% | 14% | 15% | 16% |
| Developing and implementing privacy policies and guidance | 11% | 11% | 11% | 10% |
| Performing privacy risk assessments and data inventories | 9% | 9% | 9% | 8% |
| Activities not related to privacy | 9% | 13% | 9% | 7% |
| Analyzing privacy regulations | 8% | 9% | 8% | 9% |
| Monitoring and measuring privacy compliance and enforcement | 8% | 9% | 8% | 8% |

**Government organizations actually have the longest-tenured privacy programs**

# Unregulated firms have the largest programs and the highest incidence of certified professionals

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Certifications** | | | | |
| Have a CIP* certification | 62% | 50% | 57% | 67% |
| No certification | 24% | 32% | 24% | 20% |
| **Staffing** | | | | |
| Mean number of employees dedicated to privacy | 12 | 10 | 10 | 17 |
| Expect full-time dedicated staff to increase | 31% | 23% | 34% | 30% |
| **Budget** | | | | |
| Median budget for privacy | $277,025 | $130,000 | $250,000 | $300,000 |
| Expect budget will increase | 31% | 25% | 32% | 35% |
| Less than sufficient to meet privacy needs | 59% | 70% | 60% | 52% |
| Proportion of privacy budget allocated to salary and travel | 51% | 55% | 51% | 50% |
| Proportion of privacy budget allocated to professional development | 9% | 10% | 9% | 10% |

**Unregulated firms are the most likely to have a certified decisionmaker, have more privacy employees, have larger budgets—and are the most likely to say their budget will increase even further**

# Unregulated businesses have a broader set of privacy needs and applications

## Key Differences by Industry Type

| | ALL | Gov’t | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Main Reasons for Privacy Program** | | | | |
| To meet regulatory compliance obligations | 93% | 92% | 94% | 89% |
| **To reduce risk of data breach notification/publicized data breaches** | **77%** | **70%** | **82%** | **72%** |
| **To enhance the company’s brand and public trust** | **61%** | **50%** | **61%** | **66%** |
| **To meet consumer expectations and enhance trust** | **60%** | **49%** | **63%** | **65%** |
| **To meet the expectations of business clients and partners** | **54%** | **33%** | **56%** | **61%** |
| To be good corporate citizens | 45% | 30% | 48% | 46% |
| To reduce the risk of employee and consumer lawsuits | 43% | 31% | 45% | 44% |
| **To enable global operations and entry into new markets** | **29%** | **3%** | **25%** | **40%** |
| **To provide a competitive differentiator** | **26%** | **3%** | **26%** | **39%** |
| To increase the value and quality of data | 23% | 19% | 22% | 25% |
| To increase revenues from cross-selling and direct marketing | 14% | 2% | 15% | 17% |
| To reduce the cost of storing data | 8% | 4% | 10% | 7% |

**Unregulated firms are more focused on brand, customer and business partner considerations**

# As for top two priorities, unregulated and government firms differ in a couple of respects

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Ranked in Top Two of Privacy Priorities** | | | | |
| **Regulatory and legal compliance** | **67%** | **75%** | **69%** | **59%** |
| Safeguarding data against attacks and threats | 44% | 47% | 46% | 43% |
| Increasing consumer trust | 32% | 24% | 34% | 36% |
| **Marketplace reputation and brand** | **28%** | **14%** | **31%** | **34%** |
| Ethical decision-making concerning use of data | 18% | 23% | 16% | 20% |
| Ensuring business partner compliance (including by service providers, outsourcing vendors) | 17% | 14% | 17% | 16% |
| Maintaining or enhancing the value of information assets | 10% | 9% | 9% | 12% |
| **Increasing employee trust** | **9%** | **15%** | **8%** | **8%** |

**When it comes to priorities, government agencies are strongly focused on compliance, while unregulated firms have more of a focus on their reputation in the market**

# With the exception of PIAs, government agencies are the least likely to use various privacy resources

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Internal and External Resources** | | | | |
| Have worked with privacy attorney in past year | 66% | 44% | 66% | 71% |
| **Uses internal audit for privacy audits** | **63%** | **46%** | **70%** | **60%** |
| **Have a Privacy Working Group** | **40%** | **25%** | **46%** | **39%** |
| **Have Vendor Management Program** | **63%** | **35%** | **69%** | **66%** |
| Use GRC tools | 42% | 20% | 47% | 43% |
| Have centralized Contract Management System | 35% | 37% | 35% | 32% |
| **Use Privacy Impact Assessments (PIAs)** | **59%** | **83%** | **53%** | **58%** |
| **Involved in creating privacy program** | 57% | 50% | 57% | 60% |

**Interestingly, regulated firms other than government tend to be the ones most likely to use audits, work groups, and vendor management programs**

# Key differences exist in the functions privacy professionals work with

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Interact With on a Regular Basis …** | | | | |
| Information Security | 83% | 66% | 86% | 84% |
| Legal | 79% | 69% | 80% | 78% |
| Information Technology | 72% | 63% | 72% | 71% |
| **Regulatory Compliance** | **64%** | **48%** | **73%** | **60%** |
| Human Resources | 56% | 42% | 55% | 58% |
| **Internal Audit** | **45%** | **30%** | **49%** | **45%** |
| **Marketing** | **42%** | **10%** | **42%** | **51%** |
| **Product Managers** | **40%** | **12%** | **39%** | **56%** |
| **Records Management** | **39%** | **66%** | **41%** | **24%** |

**Government agencies interact regularly with Records Management, other regulated organizations with Compliance and Audit and unregulated firms with Marketing and Product**

# However, only one key difference, for government agencies, is seen for level of influence

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Have Great Deal or Some Influence Over (top functions) . . .** | | | | |
| Information Security | 87% | 80% | 88% | 87% |
| Regulatory Compliance | 85% | 77% | 86% | 87% |
| Legal | 83% | 69% | 85% | 86% |
| Information Technology | 81% | 79% | 83% | 78% |
| Human Resources | 73% | 63% | 73% | 76% |
| Corporate Ethics | 70% | 57% | 72% | 74% |
| **Records Management** | **66%** | **77%** | **68%** | **57%** |
| Internal Audit | 65% | 66% | 65% | 65% |

**For degree of influence, only one difference emerges—government agencies and their influence on Records Management.**

# Government agencies feel they should have more say in several areas

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **SHOULD Have Great Deal or Some More Influence Over (top functions) …** | | | | |
| Information Technology | 46% | 47% | 48% | 42% |
| **Information Security** | **46%** | **57%** | **45%** | **40%** |
| Corporate Ethics | 41% | 51% | 39% | 41% |
| Human Resources | 41% | 44% | 42% | 35% |
| Product Designers | 38% | 32% | 37% | 42% |
| **Regulatory Compliance** | **37%** | **49%** | **36%** | **34%** |
| Product Managers | 37% | 31% | 36% | 40% |
| Product Engineers | 36% | 30% | 36% | 39% |
| **Physical Security** | **36%** | **42%** | **27%** | **25%** |

**Government agencies would LIKE to have more influence over several functions in their organizations**

# For accomplished initiatives, few differences exist by industry type

## Key Differences by Industry Type

| | ALL | Gov't | Other Regulated | Un-Regulated |
|---|---|---|---|---|
| **Projects Accomplished** | | | | |
| Training and awareness | 49% | 51% | 49% | 49% |
| Policy revision | 37% | 22% | 36% | 41% |
| Privacy audits and assessments | 34% | 33% | 32% | 37% |
| Vendor and third-party assurance | 33% | 23% | 31% | 36% |
| Privacy choice and consent consolidation | 32% | 25% | 32% | 36% |
| Data loss prevention technology | 31% | 25% | 34% | 29% |
| Governance, risk and compliance technology | 28% | 22% | 29% | 29% |
| Process documentation and improvement | 27% | 27% | 26% | 26% |
| Data inventorying and mapping | 26% | 18% | 25% | 29% |
| Data use logging and monitoring technology | 25% | 23% | 25% | 29% |
| **External certification** | **24%** | **16%** | **20%** | **33%** |

**The one "initiative" where we see a difference by type of industry—unregulated firms are more likely to have gotten external certification**