2011

Privacy Professional's Role, Function and Salary Survey

International Association of Privacy Professionals

iapp CANADA
international association of privacy professionals

2011
Privacy Professional's Role, Function and Salary Survey

International Association of Privacy Professionals

A Message from the IAPP

We are happy to present this year's IAPP Canada Privacy Professional's Role, Function and Salary Survey.

Our partners at Ryerson University scrutinized the information provided by all of you—IAPP Canada members—plus dozens of other privacy professionals—to bring this report to fruition. If you have been eagerly awaiting the results like we have, you can take a sneak peek on page five, where we have provided a snapshot of the typical Canadian privacy pro in both the public and private sector.

We think this report offers the most comprehensive look to date of the Canadian data protection professional of 2011. It paints a picture of who we are and what we do. With this information we can determine where we are heading, what hurdles might lie ahead and what we can do to navigate them. We thank the excellent researchers at Ryerson's Privacy and Cyber Crime Institute for bringing these findings to light.

Bringing you this picture of the Canadian profession would not have been possible without your input. To those who participated in this year's survey, thank you. We look forward to expanding it and building upon this strong foundation of knowledge in the coming years as the profession—and the professional—continues to mature.

Sincerely,

B. Bellamy

Bojana Bellamy, LLM
Chairman, IAPP

Kris Klein, CIPP/C
Managing Director, IAPP Canada

To receive a notification when the 2012 survey launches later this year, please e-mail research@privacyassociation.org.

Contents

Executive Summary

IAPP Canada and Ryerson University's Privacy and Cyber Crime Institute are pleased to present the findings of the annual survey of Canadian privacy professionals. This report provides a portrait of Canada's private- and public-sector privacy profession. The results are based on two online surveys offered to Canadian privacy professionals, including all members of IAPP Canada, over a three-week period between January and February 2011. The survey covered four major areas:

1. Salary and career information
2. Structure of current positions
3. Function and operations of privacy programs
4. Organizational and industry considerations

Ryerson University's Privacy and Cyber Crime Institute prepared two surveys in collaboration with IAPP Canada staff. In response to feedback from IAPP Canada members who completed the 2010 survey, this year's poll sought to discern the circumstances experienced by privacy professionals in the public and private sectors; the questions were modified and selected specifically to reflect these separate Canadian privacy realities. The survey was anonymous and confidential. The results were analysed at Ryerson University.

This study was designed to provide insights on several key questions:

1. What are the typical responsibilities performed by privacy professionals?
2. Where does the privacy role fit within the organization?
3. What are the compensation norms within the Canadian profession?
4. How do individual characteristics such as education, certifications and years of experience determine compensation?
5. What is the influence of industry, organization size, job scope and reporting relationships?
6. How is the privacy office staffed and budgeted; what are its top priorities, and how does it operate with other organizational functions?
7. How is privacy program success measured?

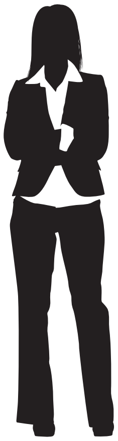
Overall Key Findings

The study's findings are detailed throughout this report under four themes: Who we are: Our privacy careers; Functions: Our roles and responsibilities; Operations: Our privacy programs, and Locations: Where we operate.

Here is a snapshot of the findings.

Characteristics of the typical Canadian privacy professional

Private Sector



- Female
- Aged 45-49
- Works in the financial services sector
- Has postsecondary education
- Might be a lawyer
- Likely to have a CIPP credential
- Has at least 20 years of work experience, with five to 15 of them spent in a privacy-related position
- Works as a senior manager or manager
- Has been in current position two to five years

Public Sector

- Almost equally likely to be female or male
- Aged 40-45
- Works within a provincial government organization
- Has postsecondary education; might have a graduate degree
- Somewhat likely to have a CIPP credential
- Has at least 20 years of work experience, with five to 15 of them spent in a privacy-related position
- Works as a manager or analyst
- Those in senior positions are likely to have more than 10 years experience, while managers or analysts are likely to have two to five years experience

Salary of the typical Canadian privacy professional

Private Sector

- Earns between $100,000 and $199,000
- Expects to receive bonus compensation based on both personal and company performance
- More than half of private-sector respondents perceive their compensation to be on a par with organizational peers, while almost half perceive their compensation to be equal to their industry peers.

Public Sector

- Earns between $75,000 and $149,000
- Significantly less than half are eligible for bonus compensation
- About half perceive their compensation to be on a par with organizational peers, while less than half perceive their compensation to be equal to their industry peers.

Other Key Findings

- The privacy role is increasingly significant to organizations.
- The privacy position is largely full-time.
- The privacy position exists relatively close to top management.
- Private- and public-sector privacy professionals have many similar priorities; however, there are some telling differences.
- Privacy programs function with modest numbers of personnel.
- There is a high level of uncertainty about future budgets.
- The majority of privacy programs do not utilize a cross-functional team approach; public-sector organizations are more likely to use cross-functional teams than are their private-sector counterparts.
- Popular success measurement techniques for privacy programs include self-assessments and audits.
- Private-sector respondents come from a wide variety of organizations, but most derive from the financial services, professional services, healthcare and IT/telecom industries.
- Public-sector respondents represent all four levels of government, with the majority operating within provincial-level organizations and about a third located within the "broader" public sector.

Survey Methods, Analysis and Limitations

Ryerson University's Privacy and Cyber Crime Institute developed two surveys in collaboration with IAPP Canada staff. The surveys addressed the different circumstances experienced by privacy professionals in the public and private sectors. Both versions of the survey were anonymous and confidential.

This report is based on an analysis of the voluntary responses provided by Canadian privacy professionals. The respondents were invited to participate via an e-mail from IAPP Canada. The invitation to participate included links to the two unique online surveys. Respondents selected the survey they thought best addressed their professional circumstances. IAPP Canada member respondents who had not consented to direct e-mail contact by the IAPP were not included in the invitation.

During a three-week period between January and February 2011, 421 recipients viewed the survey, while 214 attempted it. Those polled were presented with 50 questions of a variety of styles and lengths. All mandatory questions included an "I decline to respond" or similar response category. Ninety-three of those polled completed the survey, of which 52 percent were female and 46 percent male. Three percent declined to identify their gender. There was a 43-percent completion rate for those who completed versus those who started the survey. Analysis and writing occurred in February and March 2011.

A note about the findings:

1. For many questions, there is no significant difference between the practices of the private versus public sectors. In these circumstances, aggregate responses are provided with a brief commentary in the event of a significant difference.

2. For some questions, responses differ significantly between the sectors. In these cases, results are provided by sector.

3. Because of the difference between the number of participants who started the survey and the number who completed it, we report the sample size per question category in order to provide the greatest amount of information. On one hand, this reduces the overall utility of the results because we are unable to provide cross-tabulations on many of the questions. We provide descriptive statistics for each category.

It is not possible to determine the reasons for the differences among the rates of viewing the survey versus attempting and abandoning it versus completing the survey in its entirety. Further, these results are a single point in time—a "snapshot" of the portion of the Canadian profession that chose to participate. As a result, the findings are useful to the extent that they provide some information about privacy careers, positions, programs and organizational settings within the Canadian context. However, findings should be interpreted with caution as they are not statistically generalisable.

Survey Results

This section reports on the major findings of the 2011 Canada Privacy Professional's Role, Function and Salary Survey. Due to the inherent limitations of benchmarking methodology, the report focuses more on description and patterns and less on statistics.

The results are reported in four themes:

Theme 1: WHO WE ARE: Our privacy careers – provides an overview of the professionals according to indicators of gender, age, credentials, years of work experience, years of privacy experience, present level of responsibility, length of tenure in present position, salary and bonus and perceptions of salary equality.

Theme 2: FUNCTIONS: Our roles and positions – details the respondents' privacy positions—including where they reside in their organization by function, reporting relationship, headcount and budget—and discusses the extent of the role privacy plays in their positions.

Theme 3: OPERATIONS: Our privacy programs – explores how privacy programs are organized, looking at the size of privacy staffs and budgets and the activities for which respondents are responsible, as well as program priorities, the use of cross-functional and crisis response teams and the use of program effectiveness measures.

Theme 4: LOCATIONS: Where we operate – explains the organizational settings in which Canadian privacy professionals operate and includes information about industries/sectors, geographic scope of operations and size of organization by revenue and headcount, with a primary focus on respondents' Canadian operations.

For each section, we provide detailed findings as well as a discussion about the implications of the findings.

I. WHO WE ARE: Our Privacy Careers

This section provides a portrait of the Canadian privacy professional in 2011 and includes an overview of responses according to the career indicators of industry/sector, gender, age, credentials, years of work experience, years of privacy experience, present level of responsibility, length of tenure in present position, salary and perceptions of salary equality. Results are reported by sector to provide necessary context to these career portraits. Results are reported in aggregate and discuss any significant differences between the two sectors.

Key Findings

- The **private-sector** privacy professional is most likely a 45- to 49-year-old female working in the financial services industry. She has post-secondary education, and she might be a lawyer. She is likely to have a Certified Information Privacy Professional (CIPP) credential.
- She has at least 20 years of work experience, with five to 15 of those years spent in a privacy-related position. She works as a senior manager or manager and has been in her current position two to five years.
- Private-sector privacy pros earn in between $100,000 and $199,000 per year, and a majority expect to receive bonus compensation based on both personal performance in their positions and company performance.
- More than half of private-sector privacy professionals perceive their compensation to be on par with organizational peers, while almost half perceive their compensation to be equal to their industry peers.
- The **public-sector** privacy pro is 40- to 45 years old and could be male or female; gender was divided equally among survey respondents.
- The public-sector privacy pro works within a provincial government organization. He/she has post-secondary education and might have a graduate degree. He/she is somewhat likely to have a CIPP designation.
- He/she has at least 20 years of work experience, with five to 15 of those years spent in a privacy-related position.
- He/she works as a manager or analyst. If he/she occupies a more senior position, he/she is likely to have more than 10 years experience; if he/she is a manager or analyst, he/she is likely to have two to five years experience in the post.
- Public-sector privacy pros earn between $75,000 and $149,000 annually, and less than half are eligible for bonus compensation.
- About half of public-sector privacy pros perceive their compensation to be on par with organizational peers, while less than half perceive their compensation to be equal to their industry peers.

Detailed Findings

We report the aggregate results for industry (private sector) and level of government (public sector) as well as gender, age, credentials (education and privacy), years of work experience, years of privacy experience, present level of responsibility, length of tenure in present position, salary, bonus and perceptions of salary equality. Note that because of the difference between the number of participants who started the survey and the number who completed it, we report the sample per question category in order to provide the greatest amount of information. On one hand, this reduces the overall utility of the results because we are unable to provide cross-tabulations on many of the questions. We provide descriptive statistics for each category (sample size is given in parentheses by subheading).

Industry (n=89) (private-sector respondents only)

There were 18 industries represented within the private-sector respondent pool; however, four industries accounted for almost 60 percent of responses—financial services (24 percent), healthcare (12 percent), professional services/consulting (12 percent) and information technology (nine percent).

Level of Government (n=39) (public-sector respondents only)

All four levels of government—national, provincial, regional, municipal—were represented within the public-sector respondent pool. The provincial level accounted for almost 60 percent of respondents, followed by the federal (21 percent), regional and municipal levels (10 percent, respectively).

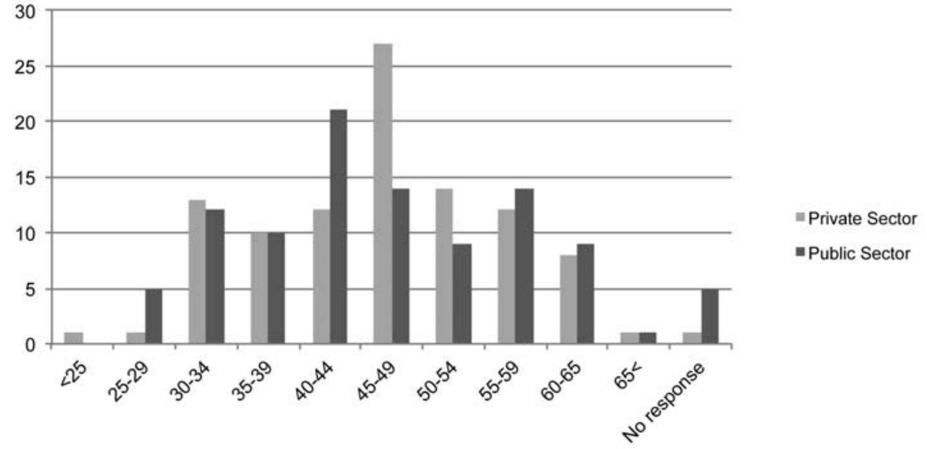
Gender (n=150)

Fifty-two percent of respondents were female; 46 percent were male. Three percent of respondents declined to identify their gender. These results approximate the gender distribution among Canadian privacy professionals. Private-sector respondents skewed slightly toward female, while the public-sector respondents were evenly split between genders.

Age (n=150)

The respondents were distributed across the age ranges. However, there was an interesting difference between the public- and private-sector samples. Twenty-seven percent of the private-sector respondents indicated that they were in the 45- to 49-year-old range, while the largest public-sector grouping was in the 40- to 44-year-old age range. However, overall, there was a fairly even distribution of respondents across all age categories despite the higher response rate from private-sector professionals.

Age distribution of respondents

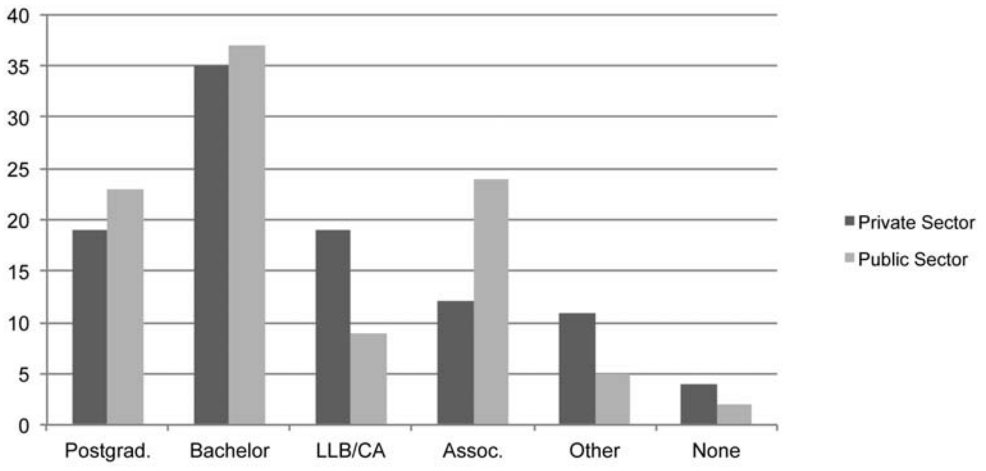


Education Credentials

Over 90 percent of all respondents have some post-secondary education. Public-sector respondents were slightly more likely (23 percent) to hold a postgraduate degree than private-sector respondents (19 percent). There was a larger presentation of lawyers and accountants (19 percent) in the private-sector sample than in the public-sector sample (9 percent).

Education credentials

(multiple responses possible)

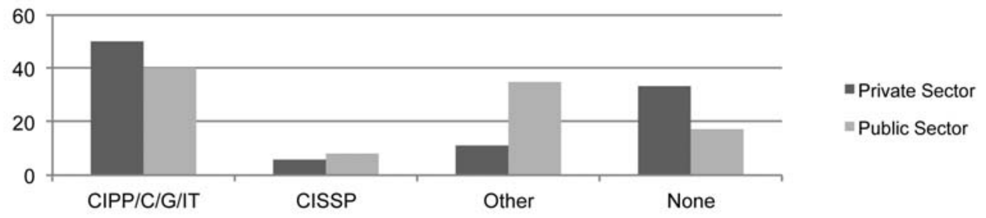


Privacy Credentials

Overall, respondents tend to seek IAPP-sanctioned privacy credentials. Half of the private-sector respondents hold a Certified Information Privacy Professional (CIPP) credential, and 40 percent of public-sector respondents make this claim.

Privacy credentials

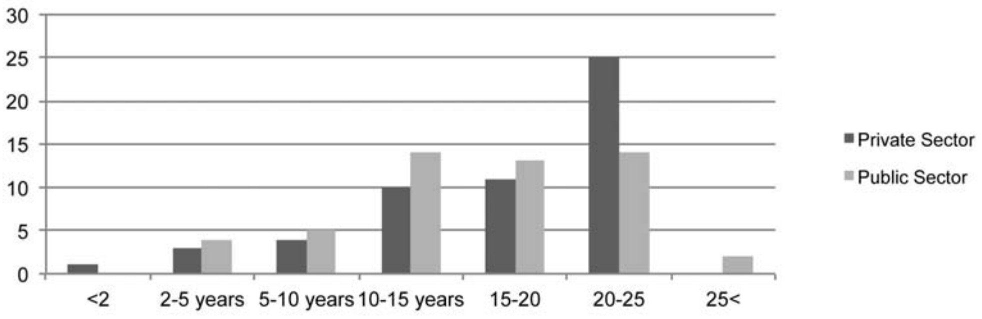
(multiple responses possible)



Work Experience

The majority of the respondents have more than 20 years of work experience. Seventy percent of private-sector respondents have 20 or more years of experience, while 64 percent of public-sector professionals fit this category. **This suggests that there are many privacy professionals potentially nearing retirement. A key issue will be adequate succession planning that will help prepare the next generation of privacy leaders.**

Work experience

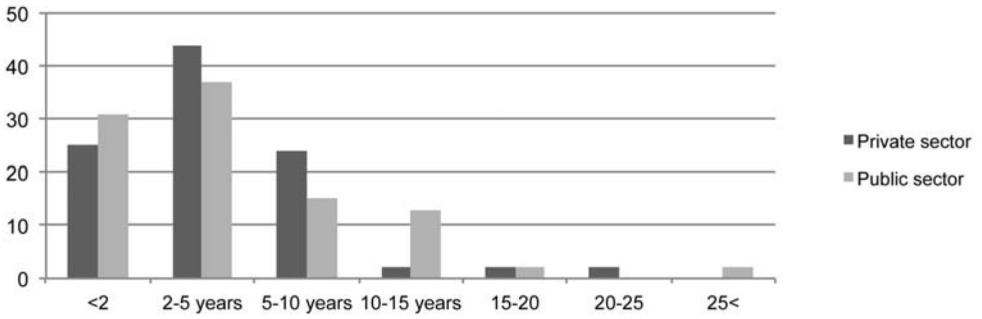


(n=146)

Years in Current Position

Both private- (44 percent) and public-sector (37 percent) respondents clustered around the "two to five years in present position" range. However, private-sector participants were more likely to have fewer than 10 years tenure in their positions (93 percent) while twice as many public servants (14 percent) had more than 10 years of experience in their positions.

Length of tenure in current position

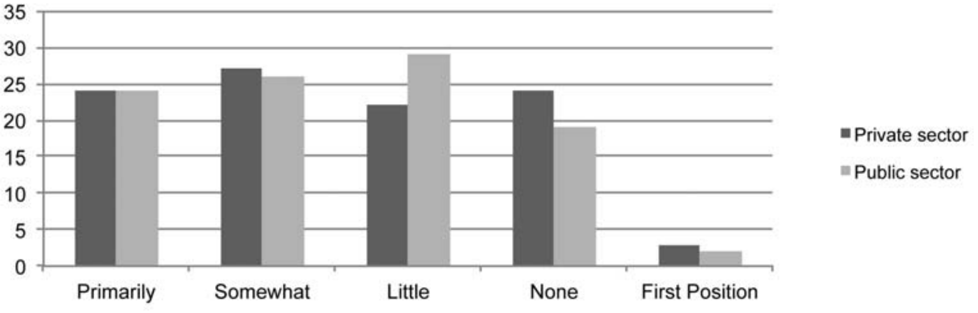


(n=123)

Prior Position

Approximately 50 percent of the positions previously held by respondents in both the private and public sectors were primarily or somewhat focussed on privacy. Private-sector respondents were equally likely to have held a previous position with only a minor (22 percent) or no (24 percent) privacy focus. In contrast, public-sector workers were 1.5 times more likely to have previously held a position with at least a minor focus (29 percent) on privacy as compared with no (19 percent) privacy responsibility. **This might suggest that there is somewhat more of a clearly defined privacy career ladder in the public sector when compared with the private sector.**

Privacy focus of previous position

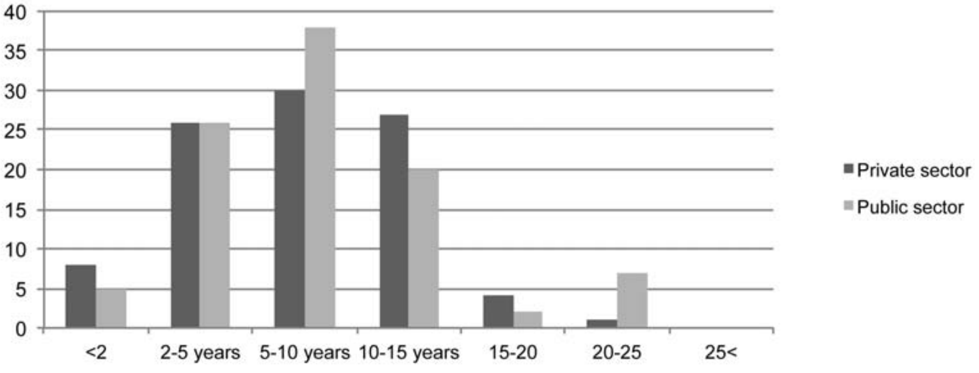


(n=150)

Privacy Experience

Overall, respondents appear to have spent a significant portion of their working lives as privacy professionals. Fifty-six percent of private-sector respondents and 58 percent of public-sector respondents have five to 15 years of privacy experience.

Privacy experience

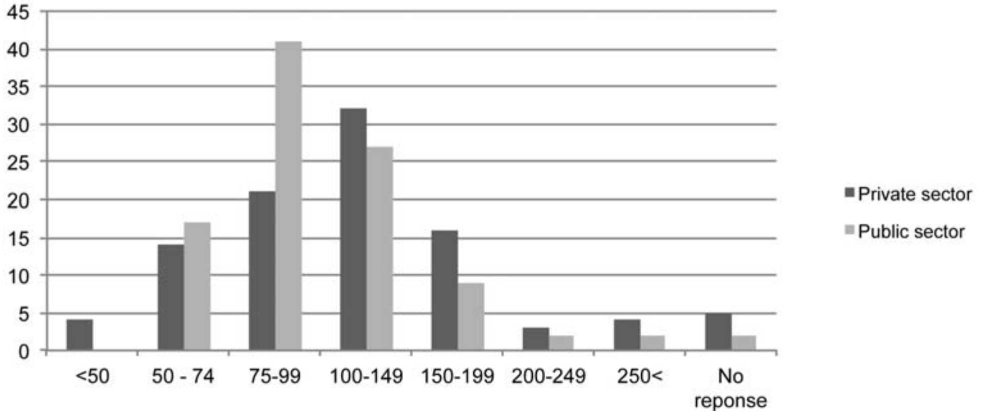


(n=150)

Salary

The salary data show a significant difference between the sectors. Almost half of the private-sector respondents indicated that they earned between $100,000 and 149,000 (31.5 percent) or $150,000 and $199,000 (16 percent). In contrast, almost 70 percent of public-sector respondents indicated they earned between $75,000 and 99,000 (41 percent) or $100,000 and 149,000 (27.5 percent).

Salary ranges

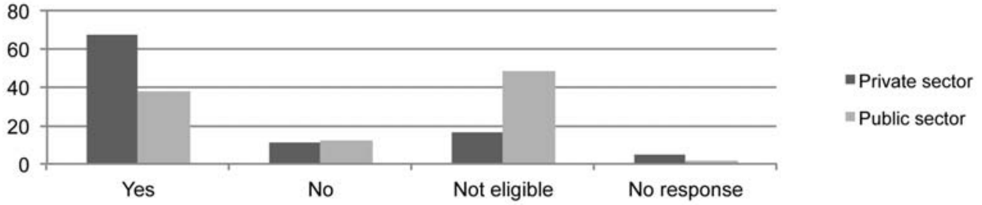


(n=150)

Annual Bonus

Approximately 33 percent of respondents indicated that this question was either not applicable to their positions or they preferred not to answer it. Perhaps not surprisingly, almost half of the public-sector respondents indicated that their positions are not eligible for a bonus payment, while this statement was applicable to 16 percent of private-sector respondents. Overall, 53 percent of respondents indicated that they expected to receive a bonus, with the private-sector respondents almost twice as likely to respond affirmatively (64 percent) than public-sector respondents (36 percent). Eleven percent indicated that they did not expect to receive a bonus.

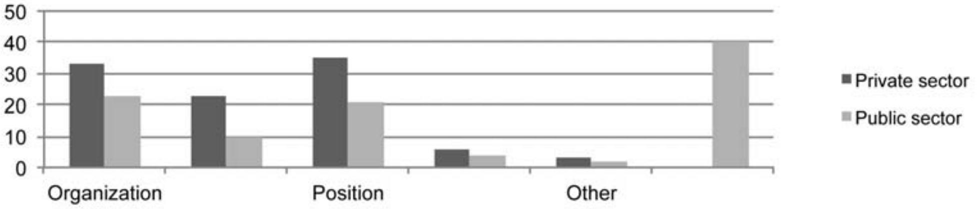
Bonus eligibility



(n=150)

Respondents indicated that the basis for receiving a bonus could be complex. Because the question was posed in a way that would provide for multiple answers, the sum was greater than 100. Interesting differences between the sectors were apparent. The two most significant reasons for receiving a bonus for private-sector respondents were for meeting the specific objectives of the position (35 percent) and overall company performance (33 percent). Business unit performance was third most important (23 percent). Of the public-sector respondents indicating that some form of bonus was applicable to their position, 23 percent reported that overall organizational performance was a key consideration, and 21 percent said that meeting their position's objectives was part of the bonus equation. Business unit performance accounted for less than 10 percent of public-sector responses.

Basis for receiving bonus

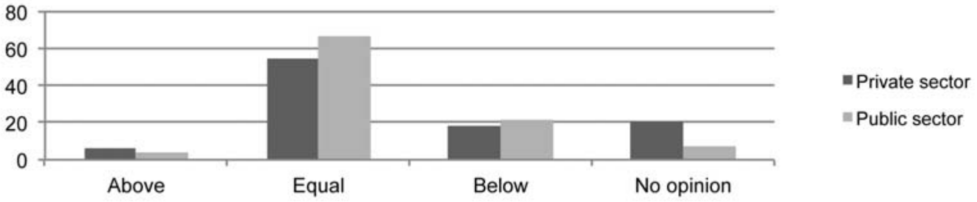


(n=150)

Compensation Comparison With Organizational Peers

Almost 80 percent of respondents reported that they perceived their compensation to be about equal to others with similar experience within their organizations. However, public-sector respondents were more likely (67 percent) to hold this view in comparison with their private-sector counterparts (55 percent). About 20 percent of each respondent group perceived their compensation to be below others with similar experience and education. Interestingly, 20 percent of private-sector respondents had no opinion, while only seven percent of public-sector respondents held this view.

Perceptions of how compensation compares to that of organizational peers

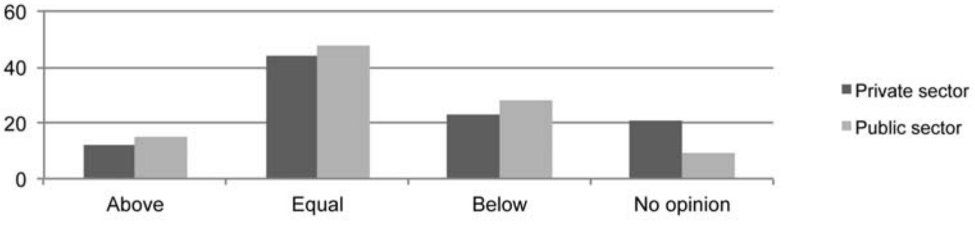


(n=150)

Compensation Comparison With Industry Peers

In contrast to how respondents feel about their compensation level as it compares to their *organizational* peers, their perceptions about how their compensation compares to *industry* peers seem to be less positive. Less than half (46 percent) of the overall respondent pool perceived their compensation to be about equal to others with similar experience within their industry. There was virtually no difference between the responses from the two sectors. Interestingly, public-sector respondents were slightly more likely (16 percent) to hold the view that they were compensated above their peers in contrast to their private-sector counterparts (12 percent). Public-sector respondents were also more likely (28 percent) than private-sector respondents (23 percent) to indicate that they perceived themselves to be not as well-compensated as their industry peers. Interestingly, more than 20 percent of private-sector respondents had no opinion, while only eight percent of public-sector respondents expressed this view.

Perceptions of how compensation compares to that of industry peers



(n=150)

At Work in the Private Sector
Kim Bustin, CIPP/C, President, Bustin Consulting

How did you become involved in the privacy field?

I first started in the privacy field more than five years ago when the crown agency I worked in at the time approached me to lead a major project to build an access and privacy program. The program needed to accommodate the organization's newly mandated compliance with four provincial privacy and access laws, in addition to PIPEDA. I was ready for a change, and this fit with my interest in project-based work, so I decided to accept the challenge. I needed to develop policies, training and procedures in a very short amount of time, so I had no choice but to immerse myself in learning the new legislation! The more I learned about access and privacy, the more I started to love it. The project was a success, and I soon became known as the access and privacy "guru" within the organization. Subsequently, I became the organization's chief privacy officer and director of risk and information management. I obtained my CIPP/C in 2009.

Please describe your current position.

Right now I'm doing what I absolutely love, and I get to be my own boss! I own my own consulting company, Bustin Consulting Limited, offering privacy and risk management services to clients across Canada. Most of my work to date has been for clients in the healthcare sector. An accomplishment I'm particularly proud of is the role I've been able to play in leading organization-wide privacy gap analysis projects for my healthcare clients in New Brunswick that are challenged to adapt their information practices to align with the province's new Personal Health Information Privacy and Access Act. I work with clients to apply the gap analysis methodology I've developed to all of their programs and systems. It is less in-depth than a PIA but more comprehensive in scope and has been very beneficial in helping clients to identify the aspects of their operations that may pose privacy risks and the changes they will need to make to be more compliant with the legislation.

If there is such a thing, what is a typical day like for you?

On a typical day, I could be at home doing a risk analysis or writing a report for a client or at a client's delivering training or interviewing the client's staff as part of a privacy gap analysis or PIA. Whatever I'm doing, I like to make sure I have lots of variety in my work. I particularly enjoy writing, and when I have time, I like to write articles, develop client proposals or contribute to the IAPP *Privacy Advisor* in my role as a member of the Publications Advisory Board. I generally have the flexibility of being able to work when and how I want, so that is a great bonus for me!

Any other thoughts you would like to share?

Being an entrepreneur in the privacy field gives me the variety I crave and provides an opportunity to work on interesting projects with some fantastic people. My career allows me to be creative in developing solutions and approaches to solving privacy challenges and provides an excellent way to continuously learn and develop in this growing field. The more I learn about privacy and data protection, the more I realize there is to know! I'm looking forward to growing my business and see a bright future ahead in the privacy field. I would highly recommend it!

II. FUNCTION: Our positions and roles

In this section, we look at respondents' privacy positions—their reporting relationships, headcounts, budgets and organizational locations. We also examine to what degree privacy is the primary role of their positions. Findings are reported by sector. Note that because of the difference between the number of participants who started the survey and the number who completed it, we report the sample per question category in order to provide the greatest amount of information. On one hand, this reduces the overall utility of the results because we are unable to provide cross-tabulations on many of the questions. We provide descriptive statistics for each category (sample size is given in parentheses by subheading).

Key Findings

- The privacy role is increasingly significant to organizations; its importance to a majority of responding organizations has increased in the past five years.
- The privacy position is largely fulltime (97 percent) with a majority of respondents spending 60 to 100 percent of their time on privacy.
- The privacy position exists relatively close to top management.
- The position is associated with core functions that protect the enterprise.
- Private-sector respondents report that their privacy position is located within the audit/compliance/risk management and legal functions. Twenty-five percent operate within "dotted line" relationships.
- Public-sector respondents report that their position is located within one of several possible functional areas including legal/ATIP/FOI, IT/security, strategy/planning/DM Office or audit/compliance/risk management. Thirty-two percent operate within "dotted line" relationships.

Detailed Findings: Private Sector

Functional Location of Position (n=71)

The majority of private-sector respondents indicated that their positions were located in audit/compliance/risk management (28 percent), legal (28 percent) or their organization's strategy/planning/office of CEO/board secretariat (10 percent). Half of these respondents' positions are not organized in a "dotted line" relationship, but 25 percent report to more than one superior, primarily someone in strategy/planning (25 percent), audit (20 percent) or information technology (15 percent).

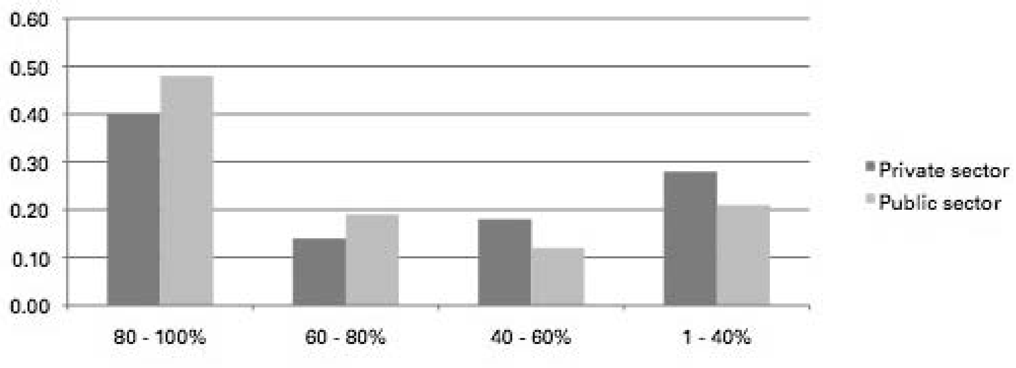
Reporting Relationships (n=71)

Twenty-eight percent of respondents indicated that their immediate superior is a senior executive ("C" level), while 27 percent report to an executive, and 25 percent report to a senior manager/director. Respondents also reported that there is variation in the number of layers between their organization's privacy leader and its highest-ranking executive. Thirty-five percent indicated that their privacy leader reports directly to the highest executive, while 42 percent report two levels below. There were three layers in 12 percent of organizations, and only 10 percent reported four layers.

Significance of Privacy Function (n=72)

Respondents were asked about the extent to which privacy was the most significant function/responsibility for their position; i.e., "how much time do you spend on privacy?" The largest group—40 percent of respondents—indicated that their privacy responsibilities take up 80 to 100 percent of their time. Interestingly, the next largest group—at 28 percent—indicated that they spend one to 40 percent of their time on privacy-related responsibilities. The rest of the respondents were likely (14 percent) to spend 60 to 80 percent of their time on privacy-related matters, while 28 percent reported spending 40 to 60 percent of their time on privacy-related matters. Those respondents who indicated that they have other "significant" responsibilities (those taking more than 10 percent of their time) reported that the responsibility areas commanding their attention are audit/compliance (25 percent), security (19 percent), legal (17 percent) and IT (14 percent).

Portion of time devoted to privacy issues



Changes to Privacy Function (n=73)

IAPP Canada was interested to learn the extent to which there had been changes to the privacy function in the past five years. The respondents were split between those who indicated that the location of the privacy function had not changed in the past five years (56 percent) and those who said that the location had changed (25 percent).

At the same time, there was overwhelming agreement (60 percent) with the statement that the "importance of the privacy position I currently occupy has increased in importance to my organization in the past five years."

Detailed Findings: Public Sector

Functional Location of Position (n=52)

The majority of public-sector respondents indicated that their positions are located in legal/ATIP/FOI (19 percent), IT/security (17 percent), audit/compliance/risk management (15 percent) and policy/program development/research (12 percent). Half of these respondents' positions are not organized in a "dotted line" relationship, but 32 percent report to more than one superior, primarily someone in legal/ATIP/FOI (17 percent), IT/security (15 percent), strategy/planning/DM office (12 percent) or audit/compliance/risk management (12 percent).

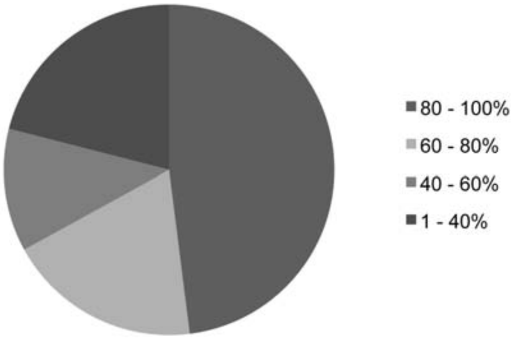
Reporting Relationships (n=52)

Twenty-nine percent of public-sector respondents indicated that their immediate superior was a senior executive (deputy or ADM level); 19 percent report to an executive, such as a director general, and 38 percent report to a senior manager/director.

Significance of Privacy Function (n=52)

Public-sector respondents were asked about the extent to which privacy was the most significant function/responsibility for their position; i.e., "how much time do you spend on privacy?" The largest group—48 percent of respondents—reported that their privacy responsibilities take up 80 to 100 percent of their time. The next largest group—at 21 percent—indicated that they spend one to 40 percent of their time on privacy-related responsibilities. The rest of the respondents were likely (19 percent) to spend 60 to 80 percent of their time on privacy-related matters, while 28 percent reported spending 40 to 60 percent. Those respondents who indicated that they have other "significant" responsibilities (those taking more than 10 percent of their time) reported that the responsibility areas commanding their attention are legal/ATIP/FOI (29 percent), policy/program development/research (14 percent), audit/compliance/risk (12 percent) and IT/security (10 percent).

Portion of time devoted to privacy issues, public sector



Changes To Privacy Function (n=52)

IAPP Canada was interested to learn the extent to which there had been changes to the privacy function in the past five years. Public-sector respondents were split on this question, with 58 percent indicating that the location of the privacy function had not changed in the past five years and 33 percent indicating that the location had changed.

At the same time, among public-sector respondents, there was overwhelming agreement (75 percent) with the statement that the "importance of the privacy position I currently occupy has increased in importance to my organization in the past five years."

III. OPERATIONS: Our privacy programs

This section describes how privacy programs are organized, looking at privacy staff size, budget, responsibilities, program priorities and the use of cross-functional and crisis response teams as well as program effectiveness measures. Findings are reported by sector. Note that because of the difference between the number of participants who started the survey and the number who completed it, we report the sample per question category in order to provide the greatest amount of information. On one hand, this reduces the overall utility of the results because we are unable to provide cross-tabulations on many of the questions. We provide descriptive statistics for each category (sample size is given in parentheses by subheading).

Key Findings

- Respondents in the private and public sectors have many similar privacy program priorities; however, there are some differences in relative emphasis.
- Privacy programs function with modest personnel (66 percent have less than five staff) and operating budgets (47 percent have annual budgets under $500,000). There is a high level of uncertainty about future budgets.
- Despite the modest resources available in general to the privacy programs, less than half of the respondents reported using cross-functional teams. Public-sector organizations are more likely to use cross-functional teams than are their private-sector counterparts.
- Organizations that use cross-functional teams find them useful for operational coordination, policy setting and awareness and promotion activities.
- Privacy programs attempt to measure their successes using a variety of techniques. The most popular techniques are very inwardly focussed, including such tools as self-assessments and audits, with only benchmarking used to compare performance against external standards.

Detailed Findings

Program Priorities

Those polled were provided with a list of 10 typical privacy program priorities and were asked to rank them in order of importance to their organizations. The single-highest program priority was "complying with laws and regulations." This was selected as the number one priority by 55 percent of private-sector respondents and 73 percent of public-sector respondents.

The table below lists the priorities by sector.

Table A: Summary of privacy program priorities*

Privacy Program Priority	Private Sector (n=53)		Public Sector (n=37)	
	Rank	%	Rank	%
Complying with laws and regulations	**1**	***55***	**1**	***73***
Managing risk	**4**	***20***	**3**	***31***
Safeguarding data against external attacks and threats	**3**	***28***	**2**	***35***
Safeguarding reputation and brand in marketplace/ safeguarding agency/ministry/organizational reputation	**2**	***33***	7	22
Safeguarding data against internal attacks and threats	**5**	***19***	**4**	***26***
Increasing consumer trust/citizen trust	6	17	**5**	***24***
Ensuring business partner compliance	6	17	8	21
Enhancing the value of information assets	7	16	9	17
Increasing employee trust	8	15	6	23
Influencing regulatory and legal frameworks	**5**	***19***	8	21

(n=90)

******Bolded italicized number indicates a "top five" priority*

The two sectors share many priorities, but they differ in the strength of the priority, as expressed by the relative placement in the priority ranking. For example, while both sectors ranked highly what could be called "security" (safeguard against threats; managing risk), more public-sector respondents ranked these as top priorities than did their private-sector counterparts. **Perhaps not surprisingly, private-sector respondents ranked safeguarding of reputation and brand in the marketplace as a higher priority (ranked second at 33 percent) than did public-sector respondents for the equivalent priority "safeguarding agency/ministry/organizational reputation," which ranked seventh at 22 percent.** Further, the private-sector respondents ranked "influencing regulatory and legal frameworks" as a top five priority (19 percent), in contrast to public-sector respondents, who placed this near the bottom.

Privacy Employee Complement (n=93)

Privacy employee complements are overwhelmingly modest regardless of sector. Sixty-six percent of respondents indicated that their complement was less than five employees. The greatest difference between sectors was that private-sector responses indicated that 55 percent had staffs of two to 10 employees, while 59 percent of public-sector respondents reported having one to four privacy employees.

In addition, respondents were asked to comment on whether they anticipated a change to the directly-related privacy headcount in the next fiscal year. Fifty-nine percent of private-sector respondents and 65 percent of public-sector respondents indicated that there would be no change. Less than 20 percent indicated an anticipated increase. Approximately 20 percent were not able to comment at the time of the survey.

Privacy Budget Overall (n=93)

Consistent with the proportion of respondents who are employed in professional consulting services or do not appear to have significant input or responsibility for their organization's privacy budget, well over 30 percent of respondents indicated that the question of the size of the dedicated privacy budget was not applicable. The remainder of responses showed that privacy program budgets are relatively modest regardless of sector. Twenty-five percent of respondents indicated they have a budget of less than $100,000, while 14 percent have budgets in the range of $100,000 to $499,000. A handful (seven percent) of respondents indicated that their privacy program budgets are in excess of $1 million.

At the time of the survey, there was a high degree of uncertainty about the direction of next year's privacy budget. Forty-one percent of private-sector respondents and 51 percent of public-sector participants were unable to say if there would be a budget change. Almost 40 percent of the overall sample thought that there would be no change, while almost 13 percent said they were expecting a budget increase.

Privacy Budget By Activity (n=93)

Respondents were asked to indicate privacy-related activities that consume at least five percent of their budgets on average. Seventeen percent indicated that this question was not applicable to their circumstances. While there was some general agreement across sectors on many activities, there are revealing differences between them, as shown in the table below. The responses were clustered by relative frequency by sector.

Table B: Private sector privacy budget categories by frequency

Privacy Program Budget Category (> 5 percent)	Private Sector (n=56)
	Cluster
Policies, procedures and governance	1 > 9 percent
Compliance monitoring	2 >8 percent
Organization awareness and training	3 >7 percent
Development and training for privacy staff Incident/breach response Professional association memberships Salaries & Benefits	4 >6 percent
Audits Communications Data inventory and mapping General overhead and administration	5 >5 percent

Table C: Public sector privacy budget categories by frequency

Privacy Program Budget Category (> 5 percent)	Public Sector (n=37)
	Cluster
Communications	1 > 11 percent
Policies, procedures and governance	2 >9 percent
General overhead and administration Organization awareness and training	3 >7 percent
Audits Development and training for privacy staff Salaries and benefits	4 >6 percent
Compliance monitoring Incident/breach response Professional association memberships	5 >5 percent

Privacy Laws (n=93)

Several respondents provide consulting services and, as a result, are not necessarily required to comply with any particular privacy statute. Because of this, we report counts of statutes and not percentages. Not surprisingly, the public-sector respondents typically are not concerned with complying with statutes of foreign jurisdictions, unlike many of their private-sector counterparts.

Consistent with the scope of Canadian and foreign operations indicated by respondents, there was a large number of different privacy statutes with which members' organizations must comply. Not surprisingly, PIPEDA topped the count (61 respondents). At the same time, a significant proportion (56 organizations) reported having to comply with health privacy legislation such as Ontario's PHIPA. Twenty-two respondents comply with the federal Privacy Act. Respondents from organizations that operate outside of Canadian jurisdiction reported that they are engaged with several privacy and privacy-related statutes, including CAN-SPAM (16 responses), Fair Credit Reporting Act (11 responses), Sarbanes-Oxley Act (12 responses), Gramm-Leach-Bliley Act (10 responses), Health Insurance Portability and Accountability Act (eight responses), Unfair and Deceptive Trade Practices (five responses) and the European Union Data Protection Directive (14 responses).

Use of Teams (n=93)

The survey asked respondents to indicate whether their organizations used a cross-functional team/steering committee to oversee the privacy function and/or activities. Interestingly, more than half (51 percent) said they did not. Public-sector respondents were more likely (40 percent) to affirm the role of a team in managing their privacy programs than their private-sector counterparts (34 percent). Approximately 12 percent reported that the concept was not applicable to their circumstances.

The following table shows the uses for a cross-functional team/steering committee by rank and by sector.

Table D: Summary of steering primary roles by sector*

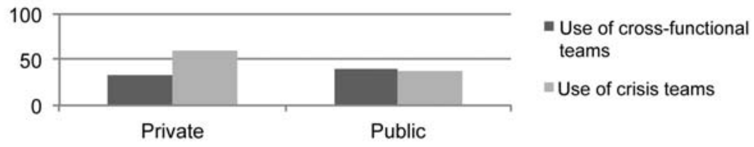
Primary Role	Private Sector (n=45)		Public Sector (n=18)	
	Rank	%	Rank	%
Awareness and promotion	**2**	***18***	***3***	***17***
Compliance monitoring	4	13	**1**	***28***
Crisis Management	4	13	4	6
Operational coordination	**1**	***20***	***2***	***13***
Policy setting	**1**	***20***	**1**	***28***
Training	***3***	***16***	4	6

**Bolded italicized number indicates a "top three" priority*

Those who responded affirmatively to the use of cross-functional teams indicated that policy setting (22 percent across the combined sample) was the top purpose. However, there were marked differences between the sectors on the importance of the other roles.

There is a striking difference between the sectors overall in their use of teams for managing privacy functions. As illustrated below, while both were somewhat likely to use cross-functional teams, private-sector respondents indicated that they were much more likely to have in place a crisis-response team than were public-sector respondents.

Use of cross-functional and crisis-response teams



Program Collaboration (n=83)

Respondents were asked to comment on how important to their organizations is privacy coordination and collaboration across functional areas. There was a high proportion of "not applicable" responses as well as "no response" (respondents had not answered the question). As a result, we report the areas of collaboration importance by sector that scored at least 40 percent in the combined rankings of 4 (important) and 5 (most important). We selected this cutoff in order to capture the differences between the sectors. These are reported in the table below, where we indicate those collaborative department/ functions.

There are several similarities between the sectors in terms collaborative groups, but their relative importance varies. For example, respondents from both sectors indicated that collaboration and cooperation with information technology/ security (almost 70 percent) was of highest importance, followed closely by legal/regulatory.

Table E: Summary of most important collaborative functions

Collaborating Function	Private Sector (n=49)		Public Sector (n=34)	
	Rank	%	Rank	%
Information Technology/Security	1	69	1	68
Legal/Regulatory (includes ATIP/FOI for public sector)	2	66	2	53
Operations/Program Management (line)	3	63	5	47
Human Resources (includes training for public sector)	4	59	6	41
Risk Management	5	56	Not included	
Records Management	6	54	Not included	
Communications/Marketing/Public Affairs	7	47	3	50
Policy/Program Development/Research	Not included		4	49
Audit/Compliance Monitoring (includes Risk Management for public sector)	9	42	5	47

Program Measurement (n=93)

Overall, 58 percent of respondents agreed that they attempt to measure their privacy programs' success. They employ a variety of approaches to gauge several different objectives. However, there are revealing differences between the sectors, as shown in the next table. The responses were clustered according to relative frequency by sector.

Table F: Summary of private sector most frequent objectives to measure

Privacy Program Objective	Private Sector (n=56)
	Cluster
Complying with policies	1 > 7 percent
Conducting employee awareness	
Avoiding data breaches	
Addressing/resolving customer/consumer complaints	2 >6 percent
Addressing/resolving data breaches	
Avoiding internal threats	
Maintaining reputation and brand image	
Mitigating risks	
Addressing/resolving employee complaints	3 >5 percent
Avoiding external threats	
Conducting annual employee awareness and knowledge reviews	
Enforcing vendor contracts	

Table G: Summary of public sector most frequent objectives to measure

Privacy Program Objective	Public Sector (n=33)
	Cluster
Addressing/resolving data breaches	1 > 9 percent
Addressing/resolving citizen/client complaints	2 >8 percent
Avoiding data breaches	
Complying with policies	
Conducting employee awareness and training	
Addressing/resolving employee complaints	3 >6 percent
Maintaining reputation	
Mitigating risks	

The degree of achievement of these various objectives was measured in a variety of ways. The top five approaches to measuring program success are reported below. Interestingly, while the ranking of the approaches differed, the private- and public-sector respondents reported similar measurement approaches overall. Both sectors rely on self-assessment as the primary measurement approach, with the public sector using informal observation equally.

Table H: Measurement approaches

Measurement Approach	Private Sector (n=56)		Public Sector (n=37)	
	Rank	%	Rank	%
Audits	2	21	2	18
Benchmarking	4	9	3	11
Informal observation	3	16	***1***	***21***
Internal case studies/after action reports	5	8	3	11
Self-assessments	***1***	***22***	***1***	***21***
Surveys	5	8	4	7

At Work in the Public Sector
Trevor Yeo, CIPP/C, Acting Manager, Investigations (PIPEDA), Office of the Privacy Commissioner

How did you become involved in the privacy field?

My involvement in the privacy field came about through my investigative experience in the insurance industry. In the United Kingdom, I worked as a complaints manager, compliance manager and anti-money laundering reporting officer. Investigations and analysis of legislation represented a fair proportion of my time, and I always found this work fascinating. I moved to Canada, and eventually found myself working for an insurance company, reviewing benefit claims for fraud and abuse. When this project ended, I thought about trying out the federal public service.

I wanted to work for a smaller agency where I could make more of a difference to Canadians and be exposed to a wide variety of challenges. The Office of the Privacy Commissioner of Canada (OPC) was looking for people with investigative experience in the private sector—so here I am! I joined the OPC in 2008, and I haven't regretted it. Privacy is an incredible field to work in, and at the OPC, we are right in the centre of things!

Please describe your current position.

I have been acting manager, investigations (PIPEDA) for about a year now. I am responsible for a team of four investigators conducting investigations into complaints against private-sector organizations. Most of my time is spent working with the investigators to ensure that we conduct impartial, timely and effective investigations into alleged contraventions of the Privacy Act and that we reach solid and consistent recommendations for the commissioner to consider.

If there is such a thing, what is a typical day like for you in the privacy field?

There is a great deal of variety in the role. In a typical day, I may discuss an investigation plan with a new investigator, talk to a CPO about a recent submission to our office, speak with a complainant about the commissioner's powers under PIPEDA, review a draft preliminary or final report with one of our case writer/analysts, discuss a legal opinion just received from a lawyer or brief the director, PIPEDA, on the status of a high-profile complaint.

Any other thoughts you would like to share?

I have noticed a shift to a more team-based, cross-branch approach in how we investigate complaints—particularly the complex ones involving technological issues such as the use of biometrics for security purposes or the practices of social networking sites. Typically, such a team will include an investigator, a lawyer, a researcher and a technology analyst. It is an inevitable step in the evolution of complaint investigations, particularly at a time when issues such as cloud computing, mobile applications and the new Canadian anti-spam legislation are in our sights.

Finally, the IAPP's CIPP/C designation is great for building up core knowledge of the field and I feel that it is important that all Canadian privacy professionals obtain this designation.

IV. LOCATIONS: Our organizational settings

This section explores the organizational settings of Canadian privacy professionals, including information about their industries/sectors, geographic scope of operations and organizational sizes by revenue and headcount. The primary focus is on respondents' Canadian operations. The findings are reported by sector. Note that because of the difference between the number of participants who started the survey and the number who completed it, we report the sample per question category in order to provide the greatest amount of information. On one hand, this reduces the overall utility of the results because we are unable to provide cross tabulations on many of the questions. We provide descriptive statistics for each category (sample size is given in parentheses by subheading).

Key Findings

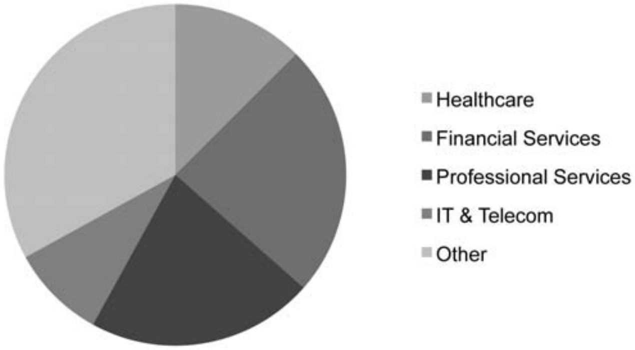
- Private-sector respondents come from a wide variety of organizations. The largest clusters are from the financial services, professional services, healthcare and IT/telecom sectors.
- The majority work in domestic firms; about one-third work in global companies.
- More than 80 percent of the firms have Canadian-based headquarters.
- Private-sector respondents' organizations are either quite large (23 percent have more than 20 locations) or quite small (52 percent have fewer than five locations).
- A "typical" private-sector organization has annual revenues of $1 million to $99 million, employs between 1,000 and 10,000 individuals and operates in 11 to 15 locations.
- Public-sector respondents represent all four levels of government, with the majority operating within provincial-level organizations and about one-third located within the "broader" public sector.
- Almost half of the public-sector respondents work in Ontario.

Detailed Findings: Private Sector

Industry Type

Private-sector respondents come from a variety of industries of which almost 40 percent are publicly traded and 34 percent are privately held. The largest clusters are in financial services (24 percent); professional services, including audit/accounting consulting and legal (21.5 percent); healthcare (12.5 percent), and IT, including software and services (9 percent). Thirty-three percent of respondents are spread across the remaining 12 industries.

Relative proportion of industries



(n=89)

Geographic Scope of Operations (n=31)

While the majority of private-sector respondents (52 percent) reported that their organizations have domestic operations only, 36 percent indicated that their organizations have a global geographic scope, operating on more than two continents. As a result, respondents' organizations have employees across the globe— in the United States (22 organizations); Latin and South America, including Mexico and the Caribbean (27 organizations); Europe (19 organizations); Asia-Pacific, including Australia and New Zealand (21), and the Middle East, including Turkey (1).

Head Office Location

While the head offices of the vast majority of respondents' organizations are located in Canada (86 percent), 13 percent indicated that their organizations' head offices are U.S.-based, and one percent listed Europe.

Dimensions of Canadian Operations

Within the domestic sphere, respondents' organizations have operations and activities in all provinces and territories. Ontario (14 percent), British Columbia (11 percent), Alberta (10 percent) and Quebec (10 percent) represent the four provinces with the most respondents. Interestingly, the count of offices/permanent locations indicated that respondents' organizations are either quite large (23 percent have more than 20 locations) or quite small (52 percent said fewer than five locations). The following table summarizes the key findings.

Table I: Dimensions of Canadian private-sector operations

Dimensions	Revenues	%	Employees	%	Locations	%
Very Large	>$1 B	21	>25,000	7	>20	23
Large	$ 100M-9999M	7	10,000-25,000	9	16-20	5
Medium	$1M-99 M	14	1,000-9,999	30	11-15	11
Small	$500,000-$1M	0	100-999	29	6-10	9
Very Small	<$500,000	8	<100	25	<5	52
No response		50		0		0

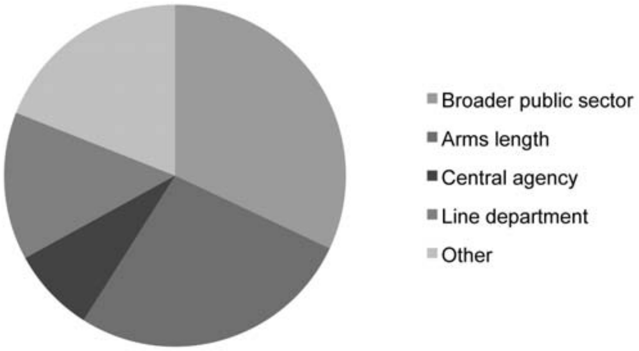
Detailed Findings: Public Sector

Level and Organizational Type

Public-sector respondents represent the range of governmental levels and types of organizations. All four levels of government (national, provincial, regional, municipal) are represented within the public-sector respondent pool. The provincial level accounts for almost 60 percent of respondents, followed by the federal (21 percent), regional and municipal levels (10 percent, respectively).

Likewise, there is a broad representation of public-sector organizational types within the respondent pool. Thirty-two percent are employed within the broader public sector (e.g., hospital or health network, school or school board, college or university) while 27 percent work in arms-length agencies or commissions. The next largest organizational type is line ministry/department (14 percent), followed by central agencies (eight percent). Nineteen percent of respondents indicate that they are employed by another type of organization, such as a municipality.

Organizational type



(n=37)

Geographic Scope And Head Office Location (n=37)

While 16 percent of respondents indicated that their employer has operations in all provinces and territories, Ontario accounts for almost half of the responses (46 percent). British Columbia, Newfoundland and Labrador, and Alberta account for 14, 10 and eight percent, respectively. At the same time, Ontario is the location of more than 60 percent of head offices for public-sector respondents, followed by BC (14 percent), Newfoundland and Labrador (11 percent), Alberta and Quebec (five percent each) and Nova Scotia (two percent).

Conclusion

Our profession continues to grow, and it is obvious from this survey that our positions continue to gain importance within the organizations for which we work. We trust you will be able to use these results not only to benchmark your own career but also to gain confidence that you belong to a strong and growing community that shares an important function in our Information Age.

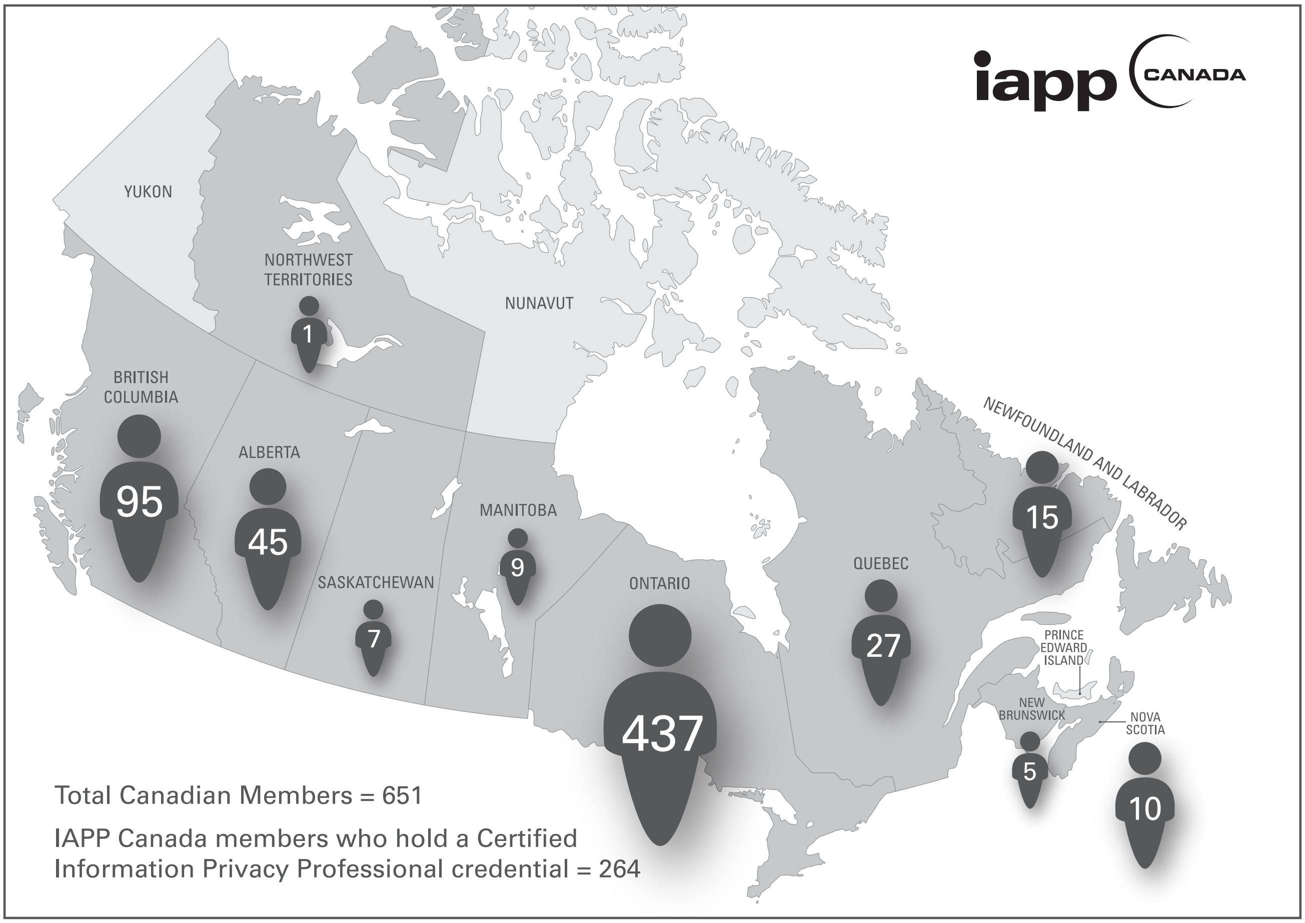
We further hope that you will continue to participate in future surveys and that you will encourage others to do so, as well. It is through the study of this information that we continue to learn and expand our careers. With more information, we can present ever richer findings.

The 2012 survey will be sent later this year. Keep an eye on the *IAPP Canada Dashboard Digest* for news of its release, or contact us at research@privacyassociation.org to be notified when it is available.

Lastly, your input on this survey and report is welcome. Please e-mail your feedback to kris@privacyassociation.org.

Appendix A: IAPP Canada Membership

Membership by Province



Total Canadian Members = 651

IAPP Canada members who hold a Certified Information Privacy Professional credential = 264

Appendix B: Survey Instrument – Public Sector

*Indicates mandatory question

Section 1: Basic Information About You

1. **What is your gender?**
   a. Female
   b. Male
   c. I prefer not to answer this question

2. **What is your age?**
   a. Over 65
   b. 60 – 65
   c. 55 – 59
   d. 50 – 54
   e. 45 – 49
   f. 40 – 44
   g. 35 – 39
   h. 30 – 34
   i. 25 – 29
   j. Under 25
   k. I prefer not to answer this question

3. **How many years have you worked in total?**
   a. More than 25 years
   b. 20 – 25 years
   c. 15 – 20 years
   d. 10 – 15 years
   e. 5 – 10 years
   f. 2 – 5 years
   g. Less than 2 years

4. **How many years of privacy experience do you have?**
   a. More than 25 years
   b. 20 – 25 years
   c. 15 – 20 years
   d. 10 – 15 years
   e. 5 – 10 years
   f. 2 – 5 years
   g. Less than 2 years

5. **Prior to assuming your present position, how would you describe your work (whether in your current organization or another one)?**
   a. Primarily focused on privacy issues
   b. Somewhat focused on privacy issues
   c. Only a little bit focused on privacy issues
   d. Previous position had nothing to do with privacy
   e. This is my first position

6. **What is your current annual salary (base pay & benefits) in Canadian dollars to the nearest $1000 using the following ranges?**
   a. Over $500,000
   b. $250,000 to $499,000
   c. $200,000 to $249,000
   d. $150,000 to $199,000
   e. $100,000 to $149,000
   f. $ 75,000 to $99,000
   g. $ 50,000 to $74,000
   h. Less than $50,000
   i. I prefer not to answer this question

7. **Do you expect to receive a bonus/merit increase this year?**
   a. Yes, I expect to receive a bonus or other special compensation
   b. Yes, I am eligible for a bonus or other special compensation but will not receive one due to organizational budget constraints
   c. No, I do not expect to receive a bonus or other special compensation
   d. No, my position is not eligible for bonus or special compensation increases OR my organization is not permitted to give bonuses or special compensation
   e. I prefer not to answer this question

8. **If you responded yes or no to the previous question (you expect/ do not expect to receive a bonus or other special compensation), please indicate the basis for which you might receive a bonus or other special compensation (check all that apply):**
   a. Not applicable
   b. Overall organizational performance
   c. Business unit performance
   d. Meeting your positions specific objectives
   e. Earning a specific credential (i.e., CIPP/C)
   f. Completing a course of education (i.e., MBA)
   g. Other

9. **I believe that the compensation I receive in relation to others in my organization is:**
   a. Above others with similar experience, education and training, and level of responsibility
   b. About equal to others with similar experience, education and training, and level of responsibility
   c. Below others with similar experience, education and training, and level of responsibility
   d. No opinion/ Not applicable

10. I believe that the compensation I receive in relation to other privacy professionals in my industry (or other peer group) is:

a. Above others with similar experience, education and training, and level of responsibility
b. About equal to others with similar experience, education and training, and level of responsibility
c. Below others with similar experience, education and training, and level of responsibility
d. No opinion/ not applicable

11. Please indicate what post-secondary degrees and/ or professional designations you have earned (check all that apply)

a. Doctorate (i.e., DBA, PhD)
b. Master (i.e., JD, LLM, MA, MBA, MSc)
c. Bachelor (i.e., BA, BComm, BEd, BSc)
d. CA/CGA/CMA/CPA
e. LLB
f. Certificate/Associate Degree (Community/Junior College)
g. None
h. Other

12. Please indicate what privacy and related designations you have earned (check all that apply):

a. CIPP/ CIPP/C /CIPP/G/ CIPP/IT
b. CIA
c. CISSP
d. CISA
e. CISM
f. None
g. Other

Section Two: Structure Of Your Privacy Position

13. What is your current position title?

14. How many years have you occupied your current position (the title of which you supplied in Question 1)?

a. More than 25 years
b. 20 – 25 years
c. 15 – 20 years
d. 10 – 15 years
e. 5 – 10 years
f. 2 – 5 years
g. Less than 2 years

15. Are you a full time employee as defined by your organization?

a. Yes
b. No

16. What organizational level best describes your current position?

a. Senior Executive (Deputy, Assistant Deputy Minister level or equivalent)
b. Executive (Director General or equivalent)
c. Senior Manager / Director
d. Manager
e. Analyst / Staff
f. Academic/researcher/educator
g. Other

17. Please indicate the functional area where the primary person you report to works:

a. Accounting/Comptroller/Financial management
b. Audit/Compliance/Program Evlauation/Risk Management
c. Communications/Marketing/Public Affairs
d. Human Resources/Organizational Development/ Training
e. Information Technology/Security
f. Legal/ATIP/FOI
g. Policy/Program Development/Research
h. Program Management (Line/Operational)
i. Strategic Planning/Office of DM/Departmental Secretariat
j. Not applicable
k. Other

18. Please indicate the organizational level of your superiors position.

a. Senior Executive (Deputy, Assistant Deputy Minister level or equivalent)
b. Executive (Director General or equivalent)
c. Senior Manager / Director
d. Manager
e. Analyst / Staff
f. Academic/researcher/educator
g. Not applicable
h. Other

19. Does your position also report to another area of the organization ("Dotted Line" relationship?)

a. Yes, I report in a dotted line relationship
b. No, my organization is not set up in this manner
c. Not applicable

20. Please indicate the functional area where the primary person you report to works:

a. Accounting/Comptroller/Financial Management
b. Audit/Compliance/Program Evaluation/Risk Management
c. Communications/Marketing/Public Affairs
d. Human Resources/Organizational Development/Training
e. Information Technology/Security
f. Legal/ATIP/FOI
g. Policy/Program Development/Research
h. Program Management (Line/Operational)
i. Strategic Planning/Office of DM/Departmental Secretariat
j. Not applicable
k. Other

21. Please indicate the organizational area of the company area where your current position is located.

a. Accounting/Comptroller/Financial Management
b. Audit/Compliance/Program Evaluation/Risk Management
c. Communications/Marketing/Public Affairs
d. Human Resources/Organizational Development/Training
e. Information Technology/Security
f. Legal/ATIP/FOI
g. Policy/Program Development/Research
h. Program Management (Line/Operational)
i. Strategic Planning/Office of DM/Departmental Secretariat
j. Not applicable
k. Other

22. To what extent is privacy the most significant aspect/responsibility of your current position? Please check the range that best reflects how much time you spend on privacy in your current position.

a. 80 – 100 %
b. 60 – 80 %
c. 40 – 60%
d. 1 – 40 %

23. In addition to your privacy-related responsibilities, what additional significant job functions (more than 10% of your time) do you perform for your organization? Please check all that apply.

a. Accounting/Comptroller/Financial Management
b. Audit/Compliance/Program Evaluation/Risk Management
c. Communications/Marketing/Public Affairs
d. Human Resources/Organizational Development/Training
e. Information Technology/Security
f. Legal/ATIP/FOI
g. Policy/Program Development/Research
h. Program Management (Line/Operational)
i. Strategic Planning/Office of DM/Departmental Secretariat
j. There is no other function that I perform
k. Other

24. Has the location (organizational area) of the privacy function changed in the last five years ?

a. Yes
b. No, the organizational area has not changed
c. No opinion
d. If yes, please indicate the previous organizational area

25. Thinking back over the past five years … I believe that the privacy position I currently occupy:

a. Has increased in importance to my organization
b. Has decreased in importance to my organization
c. Has neither increased nor decreased in importance
d. No opinion/Not applicable

Section 3: Your Current Organization

26. Please tell us what is the level of the public sector where your organization is located.

a. Federal
b. Provincial
c. Regional
d. Municipal

27. What is the geographic scope of your organization? Please check all provinces/territories in which your organization has operations.

a. All provinces and territories
b. Alberta
c. British Columbia
d. Manitoba
e. Newfoundland & Labrador
f. New Brunswick
g. Northwest Territories
h. Nova Scotia
i. Nunavut
j. Ontario
k. Prince Edward Island
l. Quebec
m. Saskatchewan
n. Yukon Territory

28. Please tell us what type is your organization.

a. Arms length agency or commission (e.g., AECL, LCBO, OFSI, TTC)
b. Broader-public sector (e.g., hospital or health network, school or school board, college or university)
c. Central Agency (e.g., Treasury Board)
d. Line ministry/department (e.g., Health, Public Works, Social Services)
e. Other

29. Please indicate the province/territory where your organization's head office is located.

a. Alberta
b. British Columbia
c. Manitoba
d. Newfoundland & Labrador
e. New Brunswick
f. Northwest Territories
g. Nova Scotia
h. Nunavut
i. Ontario
j. Prince Edward Island
k. Quebec
l. Saskatchewan
m. Yukon Territory

Section Four: Your Organizations Privacy Program

30. How many people work full time (or full time equivalent) in support of your organization's privacy function (whether directly employed by your organization or not)? Think of those people with direct, specific and significant privacy-related responsibilities. Remember to include yourself in this count!

a. More than 20 employees
b. 11 – 20 employees
c. 5 – 10 employees
d. 2 – 4 employees
e. 1 employee
f. There are no dedicated full time privacy employees

31. Do you anticipate a change to the directly-related privacy headcount in the next fiscal year ?

a. Headcount will increase
b. Headcount will decrease
c. Headcount will remain the same
d. No opinion at this point

32. Does your organization have a cross functional team steering/overseeing the privacy function/activities?

a. Yes
b. No
c. Not applicable

33. If you answered yes (your organization does use a privacy steering committee), indicate the primary roles of the steering/overseeing committee (please check all that apply):

a. Awareness & Promotion
b. Compliance monitoring
c. Crisis management
d. Operational co-ordination
e. Policy setting
f. Training
g. Other

34. Do you have a privacy crisis, privacy/security breach response team or similar group that operates only in response to a significant threat?

a. Yes
b. No
c. Not applicable

35. Please select from this list of privacy-related activities those which consume at least 5% (on average) of your budget. Check all that apply.

a. Audits
b. Communications
c. Compliance monitoring
d. Data inventory & mapping
e. Development and training for privacy staff (direct reports)
f. General overhead and administration
g. Incident/breach response
h. Legal counsel
i. Meetings with regulators/central agency staff
j. Organization awareness and training
k. Outside consultants (non-legal)
l. Policies, procedures & governance
m. Professional association memberships
n. Redress and citizen/client outreach
o. Salaries and benefits
p. Software and information technology (general office related)
q. Software and information technology (privacy/security specific)
r. Subscriptions and publications
s. Vendor management
t. Web certification and seals
u. Other
v. Not applicable given my occupation

36. What is the budget dedicated to the privacy function in your organization? Please include all the activities you checked in the previous question and select the closest range.

a. $5 million and over
b. Between $2.5 and $ 4.9 million
c. Between $1.0 and $2.4 million
d. Between $750,000 and $ 999,000
e. Between $ 500,000 and $ 749,000
f. Between $ 250,000 and $499,000
g. Between $100,000 and $ 249,999
h. Less than $ 100,000
i. Not applicable given my occupation

37. Do you expect your organization's privacy budget to change this year?

a. It will increase
b. It will decrease
c. It will stay the same
d. No opinion/Not able to tell at this juncture

38. Which privacy law(s) is(are) your organization required to observe? (Please check all that apply)

a. PIPEDA
b. Privacy Act (federal)
c. PIPA (Alberta)
d. PIPA (BC)
e. PPIPS (Quebec)
f. HIA (Alberta)
g. HIPA (Saskatchewan)
h. PHIA (Manitoba)
i. PHIPA (Ontario)
j. FIPPA (Ontario)
k. FCRA (Fair Credit Reporting Act) (USA)
l. HIPAA (Health Insurance Portability and Accountability Act) (USA)
m. GLBA (Gramm-Leach-Bliley Act) (USA)
n. COPA (Child Online Protection Act) (USA)
o. TSR (USA)
p. CAN-SPAM (USA)
q. UDTP (Unfair and Deceptive Trade Practices Act) (USA)
r. SOX (Sarbanes-Oxley Act) (USA)
s. EU Data Protection Directive
t. APEC (Asia-Pacific)
u. Australia (Asia-Pacific)
v. New Zealand (Asia-Pacific)
w. Other

39. The following is a list of typical priorities for organizational privacy programs. Please rank these according to order of importance to your firm where 1= highest priority and 10=lowest. Mark as N/A any priority that is not applicable to your organization.

	1	2	3	4	5	6	7	8	9	10	N/A
Complying with laws and regulations	□	□	□	□	□	□	□	□	□	□	□
Enhancing the value of information assets	□	□	□	□	□	□	□	□	□	□	□
Ensuring business partner compliance	□	□	□	□	□	□	□	□	□	□	□
Increasing citizen/client trust	□	□	□	□	□	□	□	□	□	□	□
Increasing employee trust	□	□	□	□	□	□	□	□	□	□	□
Influencing regulatory and legal policies/frameworks	□	□	□	□	□	□	□	□	□	□	□
Managing risk	□	□	□	□	□	□	□	□	□	□	□
Safeguarding data against external attacks and threats	□	□	□	□	□	□	□	□	□	□	□
Safeguarding data against internal attacks and threats	□	□	□	□	□	□	□	□	□	□	□
Safeguarding agency/ministry/organizational reputation	□	□	□	□	□	□	□	□	□	□	□

40. How important to your organization is privacy coordination and collaboration across functional areas? Please indicate the importance of working together to achieve privacy goals where 1=not applicable, 2=not important, 3=somewhat important, 4=important and 5=very important. For example, if your organization has a corporate social responsibility department that does not work with you at all to achieve privacy goals, you should indicate 1=not applicable. If your organization does not have a corporate social responsibility department, you should indicate N/A= not applicable.

	1	2	3	4	5	N/A	6	7	8	9	10
Accounting/Comptroller/ Financial Management	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Audit/Compliance/ Program Evaluation/Risk Management	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Communications/Marketing/ Public affairs	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Human resources/ Organizational Development/ Training	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Information Technology/ Security	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Legal/ATIP/FOI	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Policy/Program Development/Research	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Program Management (Line/ Departmental Operations)	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Strategic Planning/Office of the DM/Departmental Secretariat)	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Not Applicable	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏
Other	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏	❏

41. Does your organization attempt to measure the privacy program's success in meeting its objectives?

a. Yes
b. No
c. Not applicable

42. If you answered yes (your organization measures privacy program success), please indicate which objectives you try to measure (check all that apply):

a. Addressing/resolving citizen/client complaints
b. Addressing/resolving data breaches
c. Addressing/resolving employee complaints
d. Avoiding data breaches
e. Avoiding external threats
f. Avoiding internal threats
g. Avoiding negative media
h. Complying with policies
i. Conducting annual employee privacy awareness and knowledge reviews
j. Conducting employee privacy awareness and training
k. Enforcing vendor contracts
l. Gaining positive media coverage
m. Implementing privacy-enabling technologies
n. Increasing numbers of staff with privacy certification
o. Maintaining reputation
p. Managing budget
q. Minimizing costs associated with incident responses
r. Minimizing response times to incidents
s. Mitigating risks
t. Other

43. If you answered yes (your organization measures privacy program success), please indicate which measurement methods you use to assess the effectiveness of your privacy programs (check all that apply):

a. Audits
b. Benchmarking against other companies / industries
c. Benchmarking against other public organizations
d. Competitive intelligence
e. Cost accounting studies
f. Focus groups
g. Informal observation
h. Internal case studies / after action reports
i. "Mystery" shoppers (on and offline)
j. ROI studies
k. Self assessments
l. Surveys
m. Other

Appendix C: Survey Instrument – Private Sector

*Indicates mandatory question

Section 1: Basic Information About You

1. What is your gender?

a. Female
b. Male
c. I prefer not to answer this question

2. What is your age?

a. Over 65
b. 60 – 65
c. 55 – 59
d. 50 – 54
e. 45 – 49
f. 40 – 44
g. 35 – 39
h. 30 – 34
i. 25 – 29
j. Under 25
k. I prefer not to answer this question

3. How many years have you worked in total?

a. More than 25 years
b. 20 – 25 years
c. 15 – 20 years
d. 10 – 15 years
e. 5 – 10 years
f. 2 – 5 years
g. Less than 2 years

4. How many years of privacy experience do you have?

a. More than 25 years
b. 20 – 25 years
c. 15 – 20 years
d. 10 – 15 years
e. 5 – 10 years
f. 2 – 5 years
g. Less than 2 years

5. Prior to assuming your present position, how would you describe your work (whether in your current organization or another one)?

a. Primarily focused on privacy issues
b. Somewhat focused on privacy issues
c. Only a little bit focused on privacy issues
d. Previous position had nothing to do with privacy
e. This is my first position

6. What is your current annual salary (base pay & benefits) in Canadian dollars to the nearest $1000 using the following ranges?

a. Over $500,000
b. $250,000 to $499,000
c. $200,000 to $249,000
d. $150,000 to $199,000
e. $100,000 to $149,000
f. $ 75,000 to $99,000
g. $ 50,000 to $74,000
h. Less than $50,000
i. I prefer not to answer this question

7. Do you expect to receive a bonus/merit increase this year?

a. Yes, I expect to receive a bonus or other special compensation
b. Yes, I am eligible for a bonus or merit increase but will not receive one due to company budget constraints
c. No, I do not expect to receive a bonus or other special compensation
d. No, my position is not eligible for bonus or merit increases
e. I prefer not to answer this question

8. If you responded yes or no to the previous question (you expect/ do not expect to receive a bonus or other special compensation), please indicate the basis for which you might receive a bonus or other special compensation (check all that apply):

a. Overall company performance
b. Business unit performance
c. Meeting your positions specific objectives
d. Earning a specific credential (i.e., CIPP/C)
e. Completing a course of education (i.e., MBA)
f. Other

9. I believe that the compensation I receive in relation to others in my organization is:

a. Above others with similar experience, education and training, and level of responsibility
b. About equal to others with similar experience, education and training, and level of responsibility
c. Below others with similar experience, education and training, and level of responsibility
d. No opinion/ Not applicable

10. I believe that the compensation I receive in relation to other privacy professionals in my industry (or other peer group) is:

a. Above others with similar experience, education and training, and level of responsibility
b. About equal to others with similar experience, education and training, and level of responsibility
c. Below others with similar experience, education and training, and level of responsibility
d. No opinion/ not applicable

11. Please indicate what post-secondary degrees and/ or professional designations you have earned (check all that apply)

a. Doctorate (i.e., DBA, PhD)
b. Master (i.e., JD, LLM, MA, MBA, MSc)
c. Bachelor (i.e., BA, BComm, BEd, BSc)
d. CA/CGA/CMA/CPA
e. LLB
f. Certificate/Associate Degree (Community/Junior College)
g. None
h. Other

12. Please indicate what privacy and related designations you have earned (check all that apply):

a. CIPP/ CIPP/C /CIPP/G/ CIPP/IT
b. CIA
c. CISSP
d. CISA
e. CISM
f. None
g. Other

Section Two: Structure of Your Privacy Position

13. What is your current position title?

14. How many years have you occupied your current position (the title of which you supplied in Question 1)?

a. More than 25 years
b. 20 – 25 years
c. 15 – 20 years
d. 10 – 15 years
e. 5 – 10 years
f. 2 – 5 years
g. Less than 2 years

15. Are you a full time employee as defined by your organization?

a. Yes
b. No

16. What organizational level best describes your current position?

a. Senior Executive ("C level" equivalent)
b. Executive (Not "C level")
c. Senior Manager / Director
d. Manager
e. Analyst / Staff
f. I am an independent Consultant
g. I am an academic/researcher/educator
h. Other

17. Please indicate the functional area where the primary person you report to works:

a. Accounting/Comptroller
b. Audit/Compliance/Risk Management
c. Ethics/Corporate Social Responsibility/Public Affairs
d. Finance
e. Human Resources
f. Information Technology
g. Legal
h. Marketing
i. Research
j. Security
k. Strategy/Planning/Office of CEO/Board Secretariat
l. Training
m. Not applicable
n. Other

18. Please indicate the organizational level of your superiors position (as indicated in the previous question):

a. Senior Executive ("C level" equivalent)
b. Executive (Not "C level")
c. Senior Manager / Director
d. Manager
e. Analyst / Staff
f. Not applicable
g. Other

19. Does your position also report to another area of the organization ("Dotted Line" relationship?)

a. Yes, I report in a dotted line relationship
b. No, my organization is not set up in this manner
c. Not applicable

20. If you answered yes above (your position is in a dotted line relationship), please indicate the functional area where the "dotted line" person you report to works:

a. Accounting/Comptroller
b. Audit/Compliance/Risk Management
c. Ethics/Corporate Social Responsibility/Public Affairs
d. Finance
e. Human Resources
f. Information Technology
g. Legal
h. Marketing
i. Research
j. Security
k. Strategy/Planning/Office of CEO/Board Secretariat
l. Training
m. Other

21. In your organization, how many reporting levels exist between the privacy leader and the highest ranking executive?

a. One level (direct report)
b. Two levels
c. Three levels
d. Four levels
e. Five levels
f. Six levels
g. Seven or more levels

22. Please indicate the organizational area of the company where your current position is located.

a. Accounting/Comptroller
b. Audit/Compliance/Risk Management
c. Ethics/Corporate Social Responsibility/Public Affairs
d. Finance
e. Human Resources
f. Information Technology
g. Legal
h. Marketing
i. Operations
j. Security
k. Strategy/Planning/Office of CEO/Board Secretariat
l. Other

23. To what extent is privacy the most significant aspect/responsibility of your current position? Please check the range that best reflects how much time you spend on privacy in your current position.

a. 80 – 100 %
b. 60 – 80 %
c. 40 – 60%
d. 1 – 40 %

24. In addition to your privacy related responsibilities, what additional significant job functions (more than 10% of your time) do you perform for your organization? Please check all that apply.

a. Accounting/Comptroller
b. Audit/Compliance/Risk Management
c. Ethics/Corporate Social Responsibility/Public Affairs
d. Finance
e. Human Resources
f. Information Technology
g. Legal
h. Marketing
i. Security
j. There is no other function that I perform
k. Other

25. Has the location (organizational area) of the privacy function changed in the last five years ?

a. Yes
b. No, the organizational area has not changed
c. No opinion
d. If yes, please indicate the previous organizational area

26. Thinking back over the past five years … I believe that the privacy position I currently occupy:

a. Has increased in importance to my organization
b. Has decreased in importance to my organization
c. Has neither increased nor decreased in importance
d. No opinion/Not applicable

Section 3: Your Current Organization

27. What industry(ies) or sector(s) best define your organization? If your organization competes/ operates in more than one sector, please check all that apply. You may also write in the space "OTHER" if necessary.

a. Advertising/Communications/ Public Affairs
b. Agriculture/Food processing
c. Arts
d. Biological/Chemical/Pharmaceuticals
e. Consumer Product
f. Energy
g. Financial Services (retail & investment banking, insurance, etc.)
h. Healthcare
i. Hospitality, Leisure, Tourism
j. Information Technology/Software/Services
k. Manufacturing
l. Professional services – Audit & Accounting
m. Professional services - Consulting
n. Professional services - Legal
o. Research/polling
p. Retailing
q. Services
r. Telecommunications, cable, wireless, internet services
s. Transportation
t. Other

28. What is the geographic scope of your organization?

a. Global (operations/activities on more than two continents)
b. Transnational (operations/activities on two continents)
c. International (operations/activities in two countries on the same continent)
d. Domestic (operations in Canada only)

29. Is your company publicly traded?

a. Yes
b. No, my organization is privately held for profit
c. No, my organization is a non-traded cooperative
d. No, my organization is not-for-profit

30. Your company has employees in (check all that apply):

a. Canada
b. United States
c. Mexico
d. South America (including Caribbean)
e. Europe
f. Asia-Pacific (including Australia & New Zealand)
g. Middle East (including Turkey)

31. Please indicate where your organization's head office is located.

a. Canada
b. United States
c. Mexico
d. South America (including Caribbean)
e. Europe
f. Asia-Pacific (including Australia & New Zealand)
g. Middle East (including Turkey)

32. For your Canadian organization, please check all provinces and territories where you have operations/activities.

a. Alberta
b. British Columbia
c. Manitoba
d. New Brunswick
e. Newfoundland and Labrador
f. Northwest Territories
g. Nova Scotia
h. Nunavut
i. Ontario
j. Prince Edward Island
k. Quebec
l. Saskatchewan
m. Yukon

33. For your Canadian organization only, please indicate the number of offices/permanent work locations you operate .

a. Less than 5
b. Less than 10 but more than 5
c. Less than 15 but more than 10
d. Less than 20 but more than 15
e. More than 20

34. **What is the total headcount of your organization (Canadian operations only)?**
   a. More than 50,000 employees
   b. 25,000 – 49,999 employees
   c. 10,000 – 25,000 employees
   d. 5,000 – 9,999 employees
   e. 1,000 – 4,999 employees
   f. 500 – 999 employees
   g. 250 – 499 employees
   h. 100 – 249 employees
   i. Less than 100 employees

35. **Please indicate the range that most closely reflects the total revenues earned by your Canadian organization in 2009.**
   a. More than $10 Billion
   b. $ 1 – 9 Billion
   c. $500 to $999 million
   d. $100 to $499 million
   e. $ 50 – $ 99 million
   f. $25 - $ 49 million
   g. $1 – 24 million
   h. Less than $1 million but more than $500,000
   i. Less than $500,000
   j. Unable to provide

Section Four: Your Organizations Privacy Program

36. **How many people work full time (or full time equivalent) in support of your organization's privacy function (whether directly employed by your organization or not)? Think of those people with direct, specific and significant privacy-related responsibilities. Please refer only to your Canadian operations. Remember to include yourself in this count!**
   a. More than 20 employees
   b. 11 – 20 employees
   c. 5 – 10 employees
   d. 2 – 4 employees
   e. 1 employee
   f. There are no dedicated full time privacy employees

37. **Do you anticipate a change to the directly-related privacy headcount in the next fiscal year ?**
   a. Headcount will increase
   b. Headcount will decrease
   c. Headcount will remain the same
   d. No opinion at this point

38. **Does your organization have a cross-functional team steering/overseeing the privacy function/activities?**
   a. Yes
   b. No
   c. Not applicable

39. **If you answered yes (your organization does use a privacy steering committee), indicate the primary roles of the steering/overseeing committee (please check all that apply):**
   a. Awareness & Promotion
   b. Compliance monitoring
   c. Crisis management
   d. Operational co-ordination
   e. Policy setting
   f. Training
   g. Other

40. **Do you have a privacy crisis, privacy/security breach response team or similar group that operates only in response to a significant threat?**
   a. Yes
   b. No
   c. Not applicable

41. Please select from this list of privacy-related activities those which consume at least 5% (on average) your budget. Check all that apply.

a. Audits
b. Communications
c. Compliance monitoring
d. Data inventory & mapping
e. Development and training for privacy staff (direct reports)
f. General overhead and administration
g. Incident/breach response
h. Legal counsel
i. Meetings with regulators
j. Organization awareness and training
k. Outside consultants (non-legal)
l. Policies, procedures & governance
m. Professional association memberships
n. Redress and consumer outreach
o. Salaries and benefits
p. Software and information technology (general office related)
q. Software and information technology (privacy/security specific)
r. Subscriptions and publications
s. Vendor management
t. Web certification and seals
u. Not applicable given my occupation
v. Other

42. What is the budget dedicated to the privacy function in your organization? Please include all the activities you checked in the previous question and select the closest range.

a. $5 million and over
b. Between $2.5 and $ 4.9 million
c. Between $1.0 and $2.4 million
d. Between $750,000 and $ 999,000
e. Between $ 500,000 and $ 749,000
f. Between $ 250,000 and $499,000
g. Between $100,000 and $ 249,999
h. Less than $ 100,000
i. Not applicable given my occupation

43. Do you expect your organization's privacy budget to change this year?

a. It will increase
b. It will decrease
c. It will stay the same
d. No opinion/Not able to tell at this juncture

44. Which privacy law(s) is(are) your organization required to observe? (Please check all that apply)

a. PIPEDA
b. Privacy Act (federal)
c. PIPA (Alberta)
d. PIPA (BC)
e. PPIPS (Quebec)
f. HIA (Alberta)
g. HIPA (Saskatchewan)
h. PHIA (Manitoba)
i. PHIPA (Ontario)
j. FIPPA (Ontario)
k. FCRA (Fair Credit Reporting Act) (USA)
l. HIPAA (Health Insurance Portability and Accountability Act) (USA)
m. GLBA (Gramm-Leach-Bliley Act) (USA)
n. COPA (Child Online Protection Act) (USA)
o. TSR (USA)
p. CAN-SPAM (USA)
q. UDTP (Unfair and Deceptive Trade Practices Act) (USA)
r. SOX (Sarbanes-Oxley Act) (USA)
s. EU Data Protection Directive
t. APEC (Asia-Pacific)
u. Australia (Asia-Pacific)
v. New Zealand (Asia-Pacific)
w. Other

45. **The following is a list of typical priorities for organizational privacy programs. Please rank these according to order of importance to your firm where 1= highest priority and 10=lowest. Mark as N/A any priority that is not applicable to your organization.**

	1	2	3	4	5	6	7	8	9	10	N/A
Complying with laws and regulations	□	□	□	□	□	□	□	□	□	□	□
Enhancing the value of information assets	□	□	□	□	□	□	□	□	□	□	□
Ensuring business partner compliance	□	□	□	□	□	□	□	□	□	□	□
Increasing consumer trust	□	□	□	□	□	□	□	□	□	□	□
Increasing employee trust	□	□	□	□	□	□	□	□	□	□	□
Influencing regulatory and legal frameworks	□	□	□	□	□	□	□	□	□	□	□
Managing risk	□	□	□	□	□	□	□	□	□	□	□
Safeguarding data against external attacks and threats	□	□	□	□	□	□	□	□	□	□	□
Safeguarding data against internal attacks and threats	□	□	□	□	□	□	□	□	□	□	□
Safeguarding reputation and brand in marketplace	□	□	□	□	□	□	□	□	□	□	□

46. How important to your organization is privacy coordination and collaboration across functional areas? Please indicate the importance of working together to achieve privacy goals where 1=not applicable, 2=not important, 3=somewhat important, 4=important and 5=very important. For example, if your organization has a corporate social responsibility department that does not work with you at all to achieve privacy goals, you should indicate 1=not applicable. If your organization does not have a corporate social responsibility department, you should indicate N/A= not applicable.

	1	2	3	4	5	N/A
Corporate ethics/Social audit/Corporate social responsibility	□	□	□	□	□	□
Finance & accounting	□	□	□	□	□	□
Government/public affairs	□	□	□	□	□	□
Human resources	□	□	□	□	□	□
Information technology	□	□	□	□	□	□
Internal audit	□	□	□	□	□	□
Legal	□	□	□	□	□	□
Marketing	□	□	□	□	□	□
Mergers & acquisitions	□	□	□	□	□	□
Operations	□	□	□	□	□	□
Procurement	□	□	□	□	□	□
Project management	□	□	□	□	□	□
Public relations/communications	□	□	□	□	□	□
Records management	□	□	□	□	□	□
Regulatory compliance	□	□	□	□	□	□
Risk management	□	□	□	□	□	□
Sales	□	□	□	□	□	□
Security - information	□	□	□	□	□	□
Security - physical	□	□	□	□	□	□
Supply chain & logistics	□	□	□	□	□	□
Other	□	□	□	□	□	□

47. Does your organization attempt to measure the privacy program's success in meeting its objectives?

a. Yes
b. No
c. Not applicable

48. If you answered yes (your organization measures privacy program success), please indicate which objectives you try to measure (check all that apply):

a. Addressing/resolving customer/consumer complaints
b. Addressing/resolving data breaches
c. Addressing/resolving employee complaints
d. Avoiding data breaches
e. Avoiding external threats
f. Avoiding internal threats
g. Avoiding negative media
h. Complying with policies
i. Conducting annual employee privacy awareness and knowledge reviews
j. Conducting employee privacy awareness and training
k. Enforcing vendor contracts
l. Gaining positive media coverage
m. Implementing privacy enabling technologies
n. Increasing numbers of staff with privacy certification
o. Maintaining reputation and brand image
p. Managing budget
q. Minimizing costs associated with incident responses
r. Minimizing customer churn or turnover
s. Minimizing response times to incidents
t. Mitigating risks
u. Other

49. If you answered yes (your organization measures privacy program success), please indicate which measurement methods you use to assess the effectiveness of your privacy programs (check all that apply):

a. Audits
b. Benchmarking against other companies / industries
c. Competitive intelligence
d. Cost accounting studies
e. Focus groups
f. Informal observation
g. Internal case studies / after action reports
h. "Mystery" shoppers (on and offline)
i. ROI studies
j. Self assessments
k. Surveys
l. Other

About IAPP Canada

IAPP Canada was created in 2009 to serve the growing needs of the IAPP's Canadian membership. IAPP Canada is a community for Canadian members to exchange ideas and enrich their knowledge. It serves as a resource for the Canadian privacy community by providing services, education, networking opportunities and conferences tailored to the unique challenges and needs of Canadian privacy professionals.

About the Privacy and Cyber Crime Institute

The Privacy and Cyber Crime Institute at Ryerson University's Ted Rogers School of Management has a mandate to foster partnerships between Ryerson, the private sector and the public sector to research privacy and disseminate knowledge. The institute generates knowledge through workshops, public lectures and reports; creates an internal forum for faculty members with related interests to meet, discuss and develop their research, and serves as an external contact point for media and others interested in issues related to the institute.

About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest organization of privacy professionals, representing more than 7,400 members from businesses, governments and academic institutions across 50 countries.

The IAPP was founded in 2000 with a mission to define, support and improve the privacy profession globally through networking, education and certification. We are committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardise the designations for privacy professionals and provide education and guidance on opportunities in the field of information privacy.

The IAPP is responsible for developing and launching the first broad-based credentialing program in information privacy, the Certified Information Privacy Professional (CIPP). The CIPP remains the leading privacy certification for thousands of professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognised internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice.

IAPP

Global Headquarters, Pease International Tradeport, 75 Rochester Ave., Suite 4, Portsmouth, NH 03801 USA
+1 603.427.9200 www.privacyassociation.org/canada