The International Association of Privacy Professionals and iappANZ are pleased to present you with the first survey of our Australia, New Zealand and Asia-Pacific region membership.

Our hope is that our inaugural iappANZ Privacy Professionals Role, Function and Salary Survey will not only spotlight the privacy expertise within the region but also provide information to enhance your own work in the data protection field.

Our goal will be to build upon this first year of benchmarking to bring you even more in-depth reporting and analysis with future surveys of privacy professionals throughout the region.

We hope this report will provide you with greater insight into the work of your peers and will prove to be both useful and informative for your ongoing career development.

Sincerely,

J. Trevor Hughes, CIPP
President and CEO
IAPP

John Pane, CIPP, CIPP/IT
President
iappANZ
# Table of Contents

I. Executive Summary ................................................. 4

II. Survey Findings ..................................................... 5
   - Industry Sector .................................................. 5
   - Organisation Size .............................................. 6
   - Geographic Reach ............................................. 7
   - Role ................................................................... 8
   - Function .......................................................... 12
   - Salary ............................................................. 15

III. Survey Methodology ............................................. 17

Appendix: Survey Questions ..................................... 18
I. Executive Summary

The International Association of Privacy Professionals and iappANZ are pleased to present this first survey of privacy professionals in the Australia–New Zealand region. The 2011 iappANZ Privacy Professionals Role, Function and Salary Survey provides a first year of benchmarking that will allow for further analysis as more data is gathered in future surveys on the profession in this region. Based on the first year’s data, the points of interest below—as well as many other factors—are explored in detail in the sections that follow.

• **Respondent sectors and regions.** Responses to this inaugural survey indicated that four in every 10 Australia–New Zealand (ANZ) region privacy professionals work in various levels of government, while the telecommunications and financial services sectors also have large concentrations. Respondents also indicated that Australia is home to most of the privacy offices where ANZ privacy professionals work, reflecting the location of their parent companies. Similarly, Australian and New Zealand respondent organisations remain mostly focused on the Australian market with fewer than one-fourth doing business in the United States or Europe.

• **Organisation size and privacy programme maturity.** Those employing 5,000 or less accounted for half of respondents, suggesting that even in an era of economic uncertainty, small and medium-sized organisations see the importance of investing in privacy protection. The survey respondents also reported that they oversee privacy programs in the late-middle to mature stage of development.

• **The privacy professional.** Interesting findings have emerged with regard to seniority, reporting relationships, professional responsibilities and time allocation. Fewer than one-third of respondents occupy senior positions, and ANZ privacy professionals are situated in a number of different departments with diffuse reporting responsibilities. However, it is of note that more than one-third responded that they have at least “dotted-line” reporting responsibilities to the CEO or Executive Committee. Respondents also noted they tend to wear many hats, with policy development and regulatory compliance the two most common areas of additional responsibilities beyond their core privacy functions. ANZ privacy professionals also reported they would like to spend less time responding to incidents and analysing and advising on laws and regulations so they could have more time for developing privacy strategy and monitoring and measuring compliance.

• **Salary and promotions.** Almost 65 percent of respondents report salaries of at least $100,000, and clear majorities believe their pay is at least equal to that of peers within their organisations or privacy professionals in their business sectors. Meanwhile, about 40 percent believe they are in “career cul-de-sac,” with no obvious next avenue for promotion. It is important to note, however, that respondents did not report being dissatisfied with that lack of clarity regarding their next promotion.
II. Survey Findings

The findings are grouped into sections to paint a picture of the Australia-New Zealand privacy profession in the past 12 months, beginning with an overview of respondent organisations—including sector, size, location and maturity of the privacy program—followed by analysis of the roles, reporting structure, duties and levels of compensation of privacy professionals.

Industry Sector

In which sectors are Australia and New Zealand privacy professionals best represented? Almost 40 percent of respondents to the first 2011 iappANZ Privacy Professionals Role, Function and Salary Survey reported holding government positions at the state or federal level. It is interesting to note that these responses differed from those of respondents to the IAPP’s second European survey of privacy professionals, which included far fewer public-sector privacy professionals. The ANZ survey saw the smallest number of respondents hailing from the regulated healthcare sector.

Note: Respondents were asked to select all that applied, so percentages add to more than 100.
**Organisation Size**

Are Australian and New Zealand privacy professionals working mostly in large organisations? In 2011, the organisations employing more than 25,000 individuals accounted for fewer than 30 percent of survey respondents, indicating that in the region, privacy professionals are not employed predominantly by large organisations. Just over 30 percent of respondents reported workforces of 1,000 or less, suggesting that even in an era of worldwide economic concerns, organisations of all sizes are finding the privacy function to be a worthwhile budgetary investment.

### Organisation Headcount

<table>
<thead>
<tr>
<th>Headcount</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer than 250 employees</td>
<td>5</td>
<td>13%</td>
</tr>
<tr>
<td>250 to 500 employees</td>
<td>3</td>
<td>8%</td>
</tr>
<tr>
<td>501 to 1,000 employees</td>
<td>4</td>
<td>10%</td>
</tr>
<tr>
<td>1,001 to 5,000 employees</td>
<td>7</td>
<td>18%</td>
</tr>
<tr>
<td>5,001 to 25,000 employees</td>
<td>10</td>
<td>25%</td>
</tr>
<tr>
<td>25,001 to 75,000 employees</td>
<td>8</td>
<td>20%</td>
</tr>
<tr>
<td>More than 75,000 employees</td>
<td>3</td>
<td>8%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>40</td>
<td>100%</td>
</tr>
</tbody>
</table>

*Note: Respondents were asked to select all that applied.*
**Geographic Reach**

In terms of the extent to which global privacy considerations affect ANZ privacy professionals, all of the respondents reported working for organisations that are active in the Australian market, while 38 percent of their firms are present elsewhere in the Asia-Pacific region, with slightly more than one-third active in New Zealand. Only one-fourth reported doing business in Europe, the United States and other regions.

### Operating Territories

![Operating Territories Chart](chart.png)

*Note: Respondents were asked to select all that applied, so percentages may add to more than 100.*

The majority of respondents also reported their jurisdictions are located primarily in Australia, with most in Victoria. Very few of the privacy offices have jurisdiction in the United States or Europe, which is consistent with the overwhelmingly Australian focus of respondents’ parent organisations.

### Privacy Office Jurisdiction

![Privacy Office Jurisdiction Chart](chart.png)

*Note: Respondents were asked to select all that applied, so percentages may add to more than 100.*
Regarding the role of the privacy professional in organisations based in Australia and New Zealand, slightly less than one-third of respondents reported occupying a vice president or senior executive position. Interestingly, just over half of respondents to the IAPP’s general member survey for 2011—95 percent of whom were from North America—reported occupying the top three managerial positions.

![Organisational Level Pie Chart]

- Senior Manager/Vice President/Senior Associate: 30%
- Manager/Solicitor: 28%
- Administrative staff: 10%
- Director/Partner/General Manager: 7%
- Senior Executive: 5%
- Other: 20%
In terms of their work within their organisations, Australia and New Zealand privacy professionals are situated throughout different departments and have diffuse reporting responsibilities.

### Direct Reporting Structure

<table>
<thead>
<tr>
<th>Privacy Professional Reports to:</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO/Executive Committee</td>
<td>6</td>
<td>15%</td>
</tr>
<tr>
<td>General Counsel</td>
<td>4</td>
<td>10%</td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td>3</td>
<td>8%</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>Chief Security Officer</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>Chief Risk Officer</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>Chief Financial Officer</td>
<td>1</td>
<td>3%</td>
</tr>
<tr>
<td>Compliance/Ethics Officer</td>
<td>1</td>
<td>3%</td>
</tr>
<tr>
<td>Chief Marketing Officer</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Human Resources Officer</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Other</td>
<td>19</td>
<td>48%</td>
</tr>
<tr>
<td><strong>Director</strong></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td><strong>Partner</strong></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>Head of Compliance</strong></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>40</td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
More than one-third of privacy professionals maintain at least dotted-line reporting responsibilities to the chief executive officer or the executive committee.

### Additional Reporting Responsibilities

<table>
<thead>
<tr>
<th>Other Reporting Lines</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO/Executive Committee</td>
<td>11</td>
<td>35%</td>
</tr>
<tr>
<td>General Counsel</td>
<td>9</td>
<td>29%</td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td>7</td>
<td>23%</td>
</tr>
<tr>
<td>Chief Financial Officer</td>
<td>5</td>
<td>16%</td>
</tr>
<tr>
<td>Chief Security Officer</td>
<td>5</td>
<td>16%</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>4</td>
<td>13%</td>
</tr>
<tr>
<td>Compliance/Ethics Officer</td>
<td>4</td>
<td>13%</td>
</tr>
<tr>
<td>Section Head</td>
<td>4</td>
<td>13%</td>
</tr>
<tr>
<td>Human Resources Officer</td>
<td>3</td>
<td>10%</td>
</tr>
<tr>
<td>Chief Risk Officer</td>
<td>3</td>
<td>10%</td>
</tr>
<tr>
<td>Assistant Secretary</td>
<td>3</td>
<td>10%</td>
</tr>
<tr>
<td>Secretary</td>
<td>2</td>
<td>6%</td>
</tr>
<tr>
<td>Chief Marketing Officer</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Other</td>
<td>7</td>
<td>23%</td>
</tr>
<tr>
<td><strong>TOTAL RESPONDENTS</strong></td>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Respondents were asked to select all that applied, so percentages may add to more than 100.*
What is the next move for Australian and New Zealand privacy professionals? About four in 10 respondents indicated that they believe they are in a career cul-de-sac with no obvious next role in front of them. These 41 percent of respondents to the first iappANZ Privacy Professionals Role, Function and Salary Survey reported that a new role would need to be created for them in their promotion path, with almost half of those reporting they favour that outcome.

### Promotion Paths

<table>
<thead>
<tr>
<th>Promotion Paths</th>
<th>Most Likely Promotion</th>
<th>Desired Promotion</th>
<th>Most Likely Promotion #</th>
<th>Desired Promotion #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not sure/there would need to be a new role created</td>
<td>41%</td>
<td>18%</td>
<td>16</td>
<td>7</td>
</tr>
<tr>
<td>Senior compliance professional</td>
<td>15%</td>
<td>10%</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>Director/Partner</td>
<td>10%</td>
<td>13%</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Deputy General Counsel/General Counsel</td>
<td>5%</td>
<td>5%</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Assistant Secretary</td>
<td>5%</td>
<td>3%</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Chief Security Officer</td>
<td>3%</td>
<td>5%</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Section Head</td>
<td>3%</td>
<td>0%</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Senior lawyer</td>
<td>0%</td>
<td>0%</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td>0%</td>
<td>0%</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Secretary</td>
<td>0%</td>
<td>3%</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>N/A</td>
<td>5%</td>
<td>26%</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Other</td>
<td>13%</td>
<td>18%</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>39</strong></td>
<td><strong>39</strong></td>
</tr>
</tbody>
</table>
Function

ANZ privacy professionals’ work extends beyond their data protection and privacy duties. Policy development and regulatory compliance were the two most common areas of additional responsibility outside of privacy, but one-quarter of respondents or more said their additional responsibilities include governance, risk management, corporate law, information access or training.

Note: Respondents were asked to select all that applied, so percentages add to more than 100.
Several key tasks top the privacy agenda for ANZ professionals. In terms of time allocation, developing and implementing policies and guidance received the most responses from privacy pros, 69 percent of whom indicated that this is the primary focus of their efforts. The number two spot, at 67 percent, was analysing and advising upon laws and regulations, but one in every five respondents thought that too much time was taken up with this latter responsibility.

### Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Currently Spend Most Time on This</th>
<th>Want To Spend Most Time on This</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responding to incidents</td>
<td>41%</td>
<td>19%</td>
<td>22%</td>
</tr>
<tr>
<td>Analysing and advising upon laws and regulations</td>
<td>67%</td>
<td>46%</td>
<td>21%</td>
</tr>
<tr>
<td>Complaints management</td>
<td>38%</td>
<td>22%</td>
<td>17%</td>
</tr>
<tr>
<td>Reporting to management</td>
<td>46%</td>
<td>30%</td>
<td>16%</td>
</tr>
<tr>
<td>Developing and implementing policies and guidance</td>
<td>69%</td>
<td>59%</td>
<td>10%</td>
</tr>
<tr>
<td>Processing request for access to personal data</td>
<td>10%</td>
<td>3%</td>
<td>8%</td>
</tr>
<tr>
<td>Administration (personnel and budget)</td>
<td>13%</td>
<td>5%</td>
<td>7%</td>
</tr>
<tr>
<td>Developing and performing training and communications</td>
<td>51%</td>
<td>46%</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>Advising/consulting to the organisation</td>
<td>59%</td>
<td>54%</td>
<td>5%</td>
</tr>
<tr>
<td>Conducting/assisting audits</td>
<td>26%</td>
<td>27%</td>
<td>-1%</td>
</tr>
<tr>
<td>Participating in systems/product development</td>
<td>28%</td>
<td>30%</td>
<td>-2%</td>
</tr>
<tr>
<td>Performing risk assessments and data inventories</td>
<td>36%</td>
<td>41%</td>
<td>-5%</td>
</tr>
<tr>
<td>Monitoring and measuring compliance (enforcement)</td>
<td>46%</td>
<td>57%</td>
<td>-11%</td>
</tr>
<tr>
<td>Developing privacy strategy</td>
<td>46%</td>
<td>59%</td>
<td>-13%</td>
</tr>
</tbody>
</table>

Respondents say time is wasted on these activities

Respondents would like to spend more time on these activities

### Focus Areas

<table>
<thead>
<tr>
<th>Focus Areas for the Year Ahead</th>
<th>#</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>20</td>
<td>56%</td>
</tr>
<tr>
<td>Risk management</td>
<td>18</td>
<td>50%</td>
</tr>
<tr>
<td>Training and awareness</td>
<td>17</td>
<td>47%</td>
</tr>
<tr>
<td>Information governance</td>
<td>13</td>
<td>36%</td>
</tr>
<tr>
<td>General legal</td>
<td>8</td>
<td>22%</td>
</tr>
<tr>
<td>Security</td>
<td>6</td>
<td>17%</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>TOTAL RESPONDENTS</td>
<td>36</td>
<td></td>
</tr>
</tbody>
</table>

Fewer than half of respondents reported spending most of their time on monitoring and measuring compliance and developing privacy strategy, but these were listed as the top two areas for increased attention. However, 36 percent of respondents believe they will spend more time on compliance in 2012.

Note: Respondents were asked to select all that applied, so percentages in graphs above may add up to more than 100.
Are Australian and New Zealand privacy professionals having an impact? When asked to self-assess the maturity of their organisations' privacy programmes, ANZ respondents' results show peaks in the middle and high end of the maturity scale. More than half report that they are in maintenance mode, overseeing late-middle to mature programmes. This is a stronger result than their European and American peers reported in our other surveys. Privacy professionals in those regions reported that their programme maturity had a lower share at the top maturity level.

### Privacy Programme Maturity

<table>
<thead>
<tr>
<th>Self-Assessed Programme Maturity Level</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-stage: Privacy programme has not been established as a dedicated unit within the company.</td>
<td>4</td>
<td>10%</td>
</tr>
<tr>
<td>Early stage: Privacy programme is just starting to become staffed and organized, &lt; 2 years.</td>
<td>3</td>
<td>8%</td>
</tr>
<tr>
<td>Middle stage: Privacy programme is in existence and is starting to launch key initiatives, 2-3 years.</td>
<td>9</td>
<td>23%</td>
</tr>
<tr>
<td>Late middle stage: Privacy programme is starting to evaluate the effectiveness of key initiatives, 3-4 years.</td>
<td>6</td>
<td>15%</td>
</tr>
<tr>
<td>Mature stage: Privacy programme is in maintenance mode, focusing on program evaluation and refinement, 5+ years.</td>
<td>17</td>
<td>44%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>39</td>
<td></td>
</tr>
</tbody>
</table>


Salary

A clear majority of respondents to the first iappANZ Privacy Professionals Role, Function and Salary Survey reported positive indicators in terms of the state of compensation levels for privacy professionals in the region.

About 65 percent of those surveyed put their base salaries at more than $100,000 AUD, with one-third topping $150,000 AUD.
Responses also indicate that most Australia and New Zealand privacy professionals feel they are fairly compensated. In 2011, 69 percent reported they believe they are making as much or more than others in their company with similar qualifications, while a clear majority of 57 percent also believe their salaries are equal to or greater than their peers in other sectors.
This first survey of iappANZ members as well as IAPP members and other privacy professionals from the Asia-Pacific region was conducted in late August and early September 2011 to generate the results detailed in this report. This section explains the survey objectives, delivery and sample and outlines some limitations inherent in the process.

**Survey Objectives**

The study seeks to create baseline data to better understand the characteristics of privacy professionals in Australia, New Zealand and the Asia-Pacific region. In future surveys, we hope to show the development of the ANZ privacy profession by comparison to this year’s results and to surveys of IAPP members elsewhere in the world. The research goals were defined through lines of questioning that include:

- What promotions are privacy professionals aspiring to and likely to receive?
- How do privacy professionals spend their time fulfilling their responsibilities?
- Are there significant gaps between how privacy professionals are required to allocate their time versus how they would prefer to allocate it?
- What is the compensation level of privacy professionals?

**Survey Questions**

IAPP and iappANZ developed this survey with the goal of collecting information from privacy professionals. It is our experience that a survey must be brief if we hope to maximise completion rates, and for that reason, the survey was intentionally kept brief.

The survey questions were based upon those used in other IAPP regional surveys and the IAPP’s global survey with questions tailored specifically to a regional audience. The survey included multiple-choice, tick-box and “open” questions to elicit responses in a number of different ways.

To maintain confidentiality, the survey did not request individual or company-specific information, and salary information was requested in pay ranges rather than specific figures.

**Survey Limitations**

There are inherent limitations to the survey research that need to be carefully considered before drawing conclusions from sample findings:

- The current findings are derived from the returned surveys. It is always possible that individuals who did not participate are substantially different in terms of compensation and other job-related functions from those who completed the survey.
- Salary information is very sensitive. Therefore, the survey allowed individuals to choose a salary range in disclosing current compensation. The extrapolation of salary from a range should be considered as a potential limitation when interpreting results. Furthermore, to keep the survey concise and focused, the IAPP and iappANZ decided to omit other normatively important variables from the analysis. The extent to which omitted variables might explain salary cannot be estimated at this time.
- The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

**Survey Delivery and Sample**

The IAPP and iappANZ fielded the survey to members and privacy professionals who had opted to receive such surveys via e-mail in August 2011. The e-mails included a link to the survey questions displayed via an online survey tool. The survey was closed to responses on 8 September. Once closed, data was analysed via a Web-based tool to produce the report results.

We received a total of 39 completed surveys.
Appendix: Survey Questions

1. What is your gender?
2. What is your age?
3. How many years have you worked in total?
4. How many years of privacy experience do you have?
5. Prior to assuming your present position, how would you describe your work (whether in your current organisation 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 job
6. What is your job title?
7. What organisational level best describes your current position?
   a. Senior Executive
   b. Director/Partner/General Manager
   c. Senior Manager/Vice President/Senior Associate
   d. Manager/Solicitor
   e. Administrative staff
   f. Academic/researcher/educator
   g. n/a
   h. Other
8. Is this a full-time position?
9. Are you an employee of the organisation you provide privacy oversight for, or are you a contractor/consultant?
10. Check the primary person within your organisation to whom you report.
    a. CEO/Executive Committee
    b. Chief Financial Officer
    c. General Counsel
    d. Chief Information Officer
    e. Chief Privacy Officer
    f. Compliance/Ethics Officer
    g. Chief Marketing Officer
    h. Human Resources Officer
    i. Chief Security Officer
    j. Chief Risk Officer
    k. Other
11. In your organisation, how many reporting levels exist between the privacy leader and the highest ranking executive?
12. Please indicate any other formal or informal (dotted-line) reporting relationships you have within your organisation. Please check all that apply.
    a. CEO/Executive Committee
    b. Chief Financial Officer
    c. General Counsel
    d. Chief Information Officer
    e. Chief Privacy Officer
    f. Compliance/Ethics Officer
    g. Chief Marketing Officer
    h. Human Resources Officer
    i. Chief Security Officer
    j. Chief Risk Officer
    k. Section Head
    l. Secretary
    m. Assistant Secretary
    n. Other
13. 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 percent
    b. 60 – 80 percent
    c. 40 – 60 percent
    d. 1 – 40 percent
14. In addition to privacy-related responsibilities, what other job functions do you perform in your organisation? Please check all that apply.
    a. Assurance/Audit
    b. Corporate ethics
    c. Corporate law
    d. Corporate marketing/CRM
    e. Customer service
    f. FoI/Access to information
    g. General consulting
    h. General management
    i. Governance
    j. Government relations
    k. Human resources
    l. Information security
    m. Information technology
    n. Internal auditing
    o. Policy development
    p. Public relations
    q. Regulatory compliance
    r. Records management
    s. Risk management
    t. Training
    u. Webmaster (Website management)
    v. Other
15. What industry or business groups best define your organisation? Please check all that apply.
   a. Automotive
   b. Education
   c. Financial Services
   d. Government—Federal
   e. Government—State/Territory
   f. Healthcare
   g. Hospitality and Leisure
   h. Manufacturing
   i. Pharmaceuticals
   j. Professional Services
   k. Retailing
   l. Services
   m. Telecommunications
   n. Technology and Software
   o. Web Merchant
   p. Other

16. Your organisation has employees located in (check all that apply):
   a. Australia
   b. New Zealand
   c. Asia
   d. Europe
   e. United States
   f. Canada
   g. Africa
   h. Latin America (including Mexico)
   i. Other

17. What is the worldwide headcount of your organisation?

18. In which geographical region(s) is your privacy office located? Please check all that apply.
   a. Australia—New South Wales
   b. Australia—Queensland
   c. Australia—Western Australia
   d. Australia—South Australia
   e. Australia—Northern Territory
   f. Australia—Victoria
   g. New Zealand
   h. Asia-Pacific (including Australia and New Zealand)
   i. Asia
   j. Europe
   k. United States
   l. Canada
   m. Latin America (including Mexico)

19. What is the geographic scope of your organisation?
   a. Operations/activities on more than two continents
   b. Operations/activities on two continents
   c. Operations/activities on one continent

20. Is your organisation publicly traded?

21. Please indicate the range that most closely reflects the total revenues earned by your organisation in 2010.
   a. More than $10 billion
   b. $1 to 9 billion
   c. $500 to $999 million
   d. $100 to $499 million
   e. $50 to $99 million
   f. $25 to $49 million
   g. $1 to 24 million
   h. Less than $1 million but more than $500,000
   i. Less than $500,000
   j. Unable to provide
   k. N/A Government agency

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

23. Thinking back over the past five years, I believe that the privacy position I currently occupy:
   a. Has increased in importance to my organisation
   b. Has decreased in importance to my organisation
   c. Has neither increased nor decreased in importance
   d. No opinion/Not applicable

24. Please indicate the maturity stage of your company’s privacy program. Select the option that in your opinion best describes the activities associated with your company’s privacy office or initiatives.
   a. Pre-stage: Privacy program has not been established as a dedicated unit within the company.
   b. Early stage: Privacy program is just starting to become staffed and organized. < 2 years.
   c. Middle stage: Privacy program is in existence and is starting to launch key initiatives. 2-3 years
   d. Late middle stage: Privacy program is starting to evaluate the effectiveness of key initiatives. 3-4 years
   e. Mature stage: Privacy program is in maintenance mode, focusing on program evaluation and refinement. 5 years +

25. What skills or knowledge gaps currently exist, if any, that you would need to fill in order to achieve the next level of program maturity?
26. If you were to advance within your own organisation, which role would you most likely be promoted to?
   a. Deputy General Counsel/General Counsel
   b. Senior lawyer
   c. Senior compliance professional
   d. Director/Partner
   e. Chief Privacy Officer
   f. Chief Security Officer
   g. Secretary
   h. Assistant Secretary
   i. Section Head
   j. Not sure/there would need to be a new role created
   k. n/a
   l. Other

27. If you were to advance within your own organisation, which role would you ultimately aspire to?
   a. Deputy General Counsel/General Counsel
   b. Senior lawyer
   c. Senior compliance professional
   d. Director/Partner
   e. Chief Privacy Officer
   f. Chief Security Officer
   g. Secretary
   h. Assistant Secretary
   i. Section Head
   j. Not sure/there would need to be a new role created
   k. n/a
   l. Other

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

29. What is the budget dedicated to the privacy function in your organisation? Please select the closest range.

30. Do you anticipate a change in the next fiscal year to the number of employees with direct, significant privacy-related responsibilities?

31. Does your organisation have a cross-functional team steering/overseeing the privacy function/activities?

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

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

34. Do you expect your organisation’s privacy budget to change this year?

35. How many hours each week, on average, do you devote to privacy-related responsibilities?

36. What percentage of your average work week do those hours represent?

37. The following list contains numerous core activities that typically are conducted by privacy professionals within an organisation. Please check those that you currently spend most of your time on.
   a. Developing privacy strategy
   b. Analysing and advising upon laws and regulations
   c. Performing risk assessments and data inventories
   d. Developing and implementing policies and guidance
   e. Developing and performing training and communications
   f. Monitoring and measuring compliance (enforcement)
   g. Reporting to management
   h. Administration (personnel and budget)
   i. Advising/consulting to the organisation
   j. Responding to incidents
   k. Complaints management
   l. Processing request for access to personal data
   m. Participating in systems/product development
   n. Conducting/assisting audits
   o. Other
38. From the following list of numerous core activities that typically are conducted by privacy professionals within an organisation, please check those that you believe you should be spending most of your time on.
   a. Developing privacy strategy
   b. Analysing and advising upon laws and regulations
   c. Performing risk assessments and data inventories
   d. Developing and implementing policies and guidance
   e. Developing and performing training and communications
   f. Monitoring and measuring compliance (enforcement)
   g. Reporting to management
   h. Administration (personnel and budget)
   i. Advising/consulting to the organisation
   j. Responding to incidents
   k. Complaints management
   l. Processing request for access to personal data
   m. Participating in systems/product development
   n. Conducting/assisting audits
   o. Other

39. Do you envision your responsibilities changing in the next year or two?

40. In which of these areas will you be spending more time in the coming year? Please check all that apply.
   a. Compliance
   b. Risk management
   c. Security
   d. Information governance
   e. General legal
   f. Training and awareness
   g. Other

41. My current salary (base pay excluding superannuation) is within the following range:
   a. Less than $40,000 AUD
   b. Less than $40,000 NZD
   c. Between $40,000 and $50,000 AUD
   d. Between $40,000 and $50,000 NZD
   e. Between $50,001 and $75,000 AUD
   f. Between $50,001 and $75,000 NZD
   g. Between $75,001 and $100,000 AUD
   h. Between $75,001 and $100,000 NZD
   i. Between $100,001 and $150,000 AUD
   j. Between $100,001 and $150,000 NZD
   k. Between $150,001 and $200,000 AUD
   l. Between $150,001 and $200,000 NZD
   m. Between $200,001 and $300,000 AUD
   n. Between $200,001 and $300,000 NZD
   o. More than $300,000 AUD
   p. More than $300,000 NZD

42. As part of your remuneration do you expect to receive stock options, warrants or shares in 2011?

43. If you expect to receive a bonus as part of your annual compensation in 2011, what percentage of your annual income would this typically represent?

44. If you responded yes to the previous question, indicate what will most likely determine your bonus this year. Please check all that apply.
   a. Overall company performance
   b. Performance of your business unit
   c. Meeting your specific objectives
   d. Earning a specific credential (i.e., CIPP)
   e. Completing a course of education (i.e., MBA)
   f. Other

45. Please express your belief about your compensation relative to others within your company. My compensation is:
   a. Above others with similar experience, education and training within my company
   b. About equal to others with similar experience, education and training within the company
   c. Below others with similar experience, education and training within my company
   d. Other

46. How do you feel your income level is compared with your peers in other sectors?
   a. Similar
   b. Higher than my peers in other sectors
   c. Lower than my peers in other sectors
   d. Other
47. The following is a list of typical priorities for organisational privacy programs. Please rank these according to order of importance to your organisation where 1 equals the highest priority and 10 denotes the lowest. Mark as N/A any priority that is not applicable to your organisation.

<table>
<thead>
<tr>
<th>Priority</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>n/a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complying with laws and regulations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhancing the value of information assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensuring business partner compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increasing consumer trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increasing employee trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Influencing regulatory and legal frameworks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managing risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safeguarding data against external attacks and threats</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safeguarding data against internal attacks and threats</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safeguarding reputation and brand in marketplace</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
48. How important to your organisation is privacy coordination and collaboration across functional areas?
Please indicate the importance of working together to achieve privacy goals where 1 equals very important, 2 equals important, 3 is somewhat important, 4 equals important and 5 is not important. Where no cross-area collaboration is required select n/a.

<table>
<thead>
<tr>
<th>Function</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>n/a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate ethics/Social audit/Corporate social responsibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance &amp; accounting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government/public affairs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal audit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mergers &amp; acquisitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procurement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public relations/communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sales</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security—information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security—physical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply chain &amp; logistics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
49. Does your organisation attempt to measure the privacy program’s success in meeting its objectives?

50. If you answered yes (your organisation 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

51. If you answered yes (your organisation 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. Control testing
   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
About iappANZ

The International Association of Privacy Professionals—Australia and New Zealand (iappANZ) is a community of privacy professionals eager to meet, share and learn. It’s the place to engage with a regional and global network of people who are the privacy community. More than just a professional association, iappANZ provides a home for privacy professionals to learn and enrich their careers and share experiences.

About the IAPP

The International Association of Privacy Professionals (IAPP) is the world’s largest organisation of privacy professionals, representing more than 8,000 members from businesses, governments and academic institutions across 70 countries.

The IAPP was founded in 2000 with a mission to define, support and improve the privacy profession 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, standardize 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 organisations.

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.

The 2011 iappANZ Privacy Professionals Role, Function and Salary Survey analysis was executed by Jay Cline, CIPP, and Minnesota Privacy Consultants.

To participate in future IAPP research efforts, please contact us at research@privacyassociation.org.