www.pwc.com

IIA-Australia (NSW)

Digital Trust

Considering Privacy in your Risk Landscape

August 2014

pwc

Agenda

Introduction

Grace Guinto – Data Protection & Privacy capability lead

- Recently **relocated back to the PwC Melbourne practice** from the PwC Southern California market, where I worked in the Los Angeles office since 2004.
- I support organisations in managing their risks and designing privacy and information security programs and systems that **protect the data they collect, use, store, and destroy.**
- Guided organisations through the process of **understanding and responding to regulatory actions** issued by regulators such as the U.S. Federal Trade Commission, Australian Privacy Commissioner and Australian Prudential Regulatory Authority (APRA).
- I work collaboratively with organisations to create and improve sustainable information security and privacy programs to comply with regulatory actions and/or alignment with business goals. Key clients include: **Facebook, Comcast-NBC Universal, ResMed, Telstra**, **Department of Early Education & Childhood Development (Victoria).**
- Certified in industry leading privacy and security disciplines:
    - Certified Information Privacy Professional (CIPP/US)
    - Certified Information Privacy Manager (CIPM)
    - Certified Information Systems Auditor (CISA)

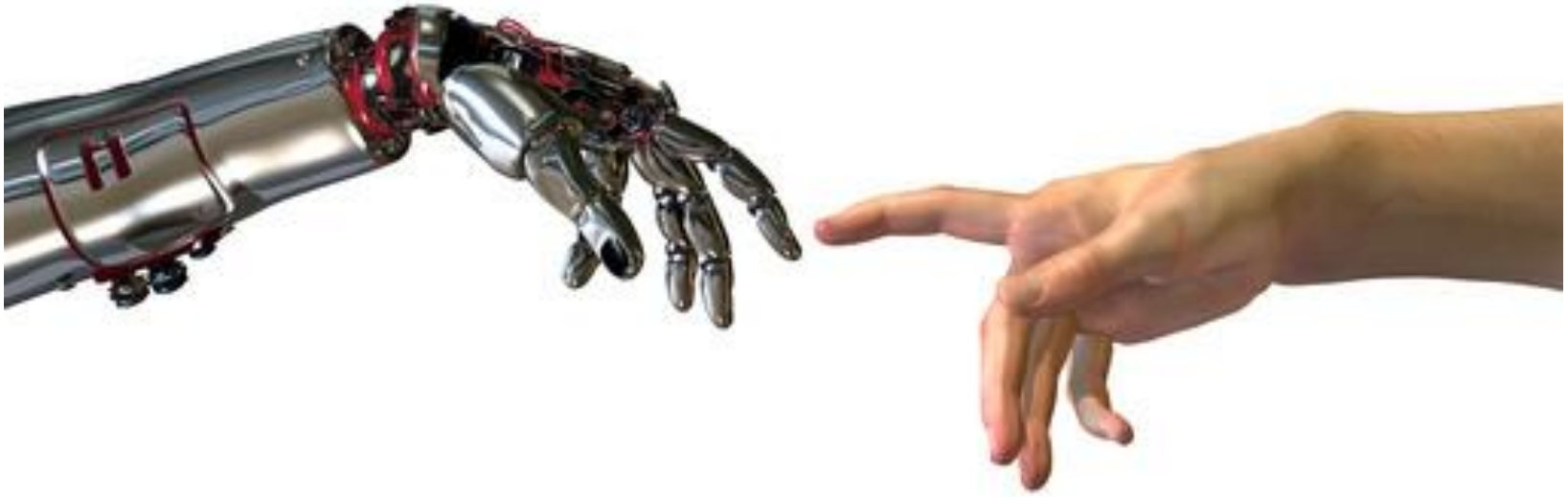
Setting the scene

1

2014 State of the internal audit profession study

- Over 1900 respondents:
  - 1400+ **CAEs** including Internal Audit managers
  - 500+ **stakeholders** (Board and Audit Committee Members, CFOs, CROs, CCOs, etc.)
- Over 100 Australian participants
- Over 125 stakeholder and CAE interviews, including **key regulators** across the globe to understand their expectations of internal audit

We're in a decade of digital change, and as Internal Audit professionals we need to evolve to keep up..

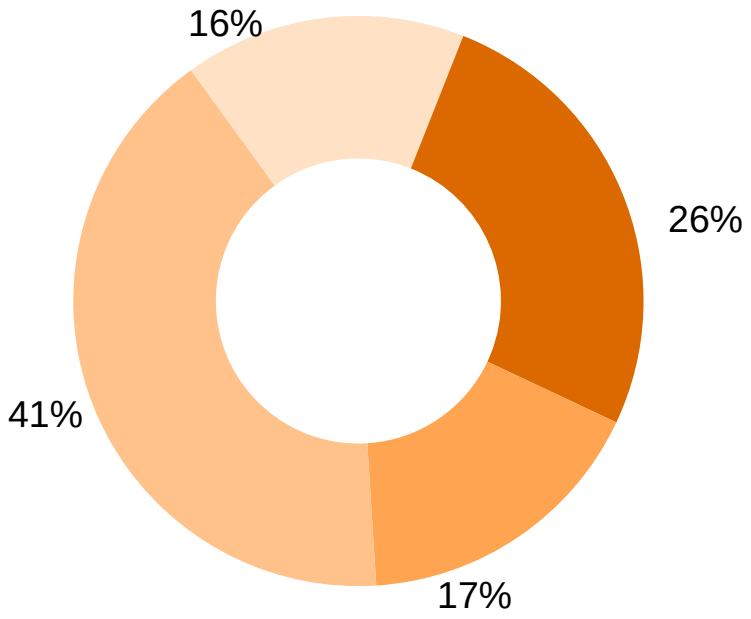


... More than ever before, our relevance to our organisations depends on our ability to embrace the new digital trust dynamic.

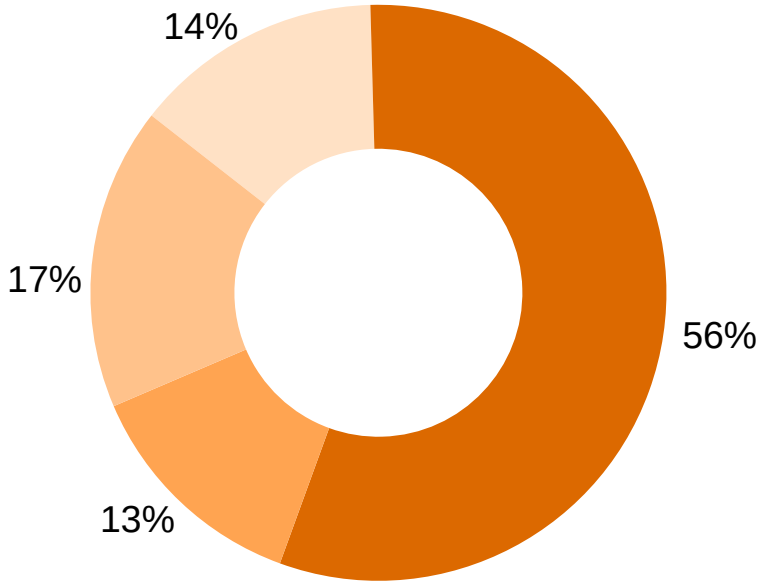
Expanding expectations of Internal Audit's value

Digital Assurance and Trust

Assurance Provider



Trusted Advisor



significant value

some value and performs well

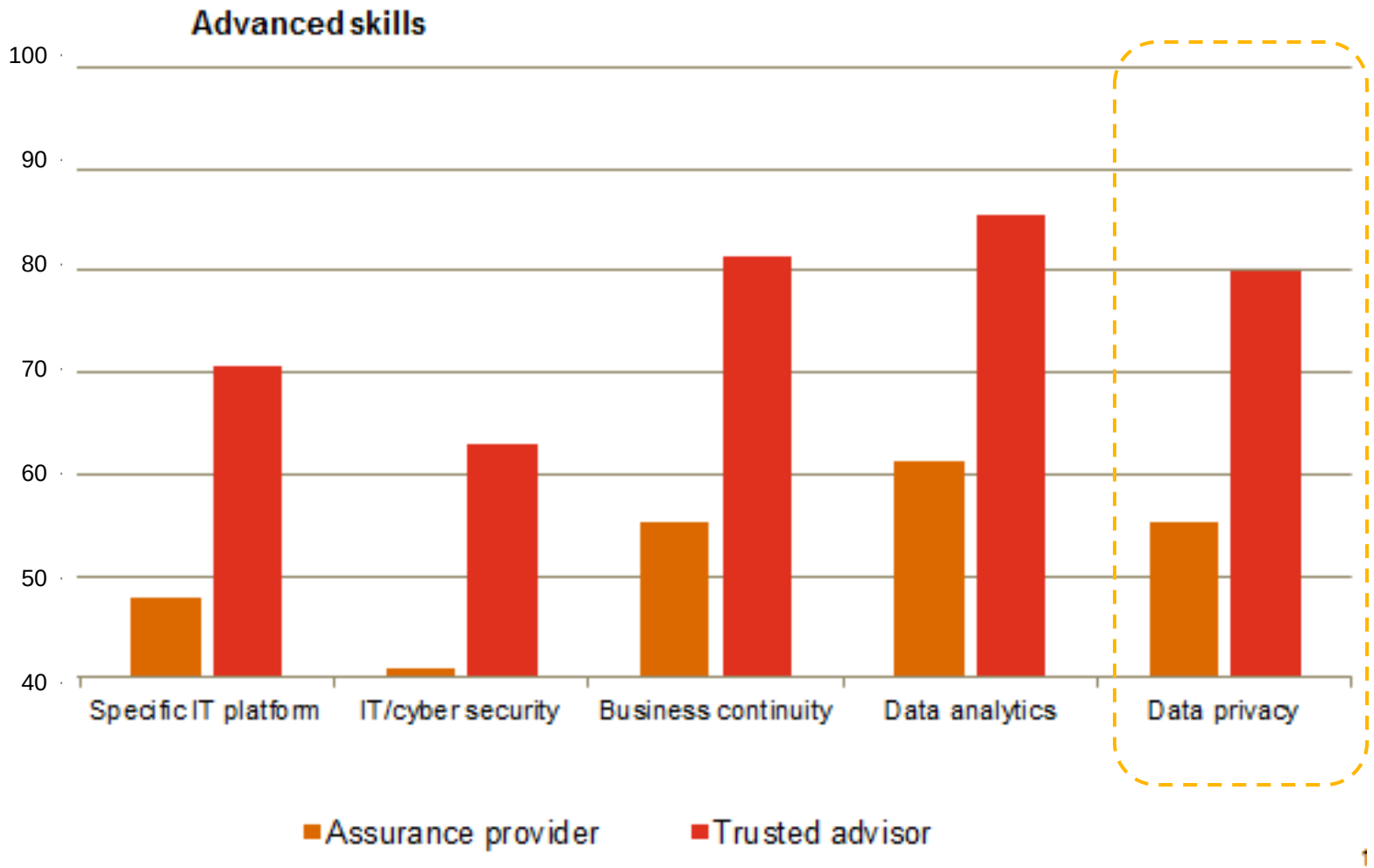
value but performs poorly

little value

Customers and the community that your organisations serve are more willing to provide personal information

With the expectation that organisations will be accountable for its safekeeping

Building the capabilities to deliver on expectations



Privacy 101

Questions for discussion

- *Is privacy one of the top 10 risks or initiatives at your organisation?*
- *In your view, why is your organisation focused on privacy risk?*

Is privacy one of the top 10 risks or initiatives at your organisation?

Votes Received: 790

A. Yes – top 5

42.7%

B. Yes – 6-10

38.4%

C. Not in the top 10

19%

Source: PwC US Data Protection and Privacy webcast, "Tomorrow's Privacy - Balancing Commitments with Business Innovation“ (Feb 2012)

In your view, why is your organisation focused on privacy risk?

Votes Received: 805

A. For legal compliance reasons/to avoid fines and penalties

12.7%

B. To maintain our reputation/brand

9.9%

C. Both compliance and brand maintenance

67.7%

D. Other reasons

4.2%

E. We're not too focused on it yet

5.5%

Source: PwC US Data Protection and Privacy webcast, "Tomorrow's Privacy - Balancing Commitments with Business Innovation“ (Feb 2012)

Questions for discussion

Has your organisation conducted and documented a comprehensive risk assessment on the topics of privacy and information security?

Has your organisation conducted and documented a comprehensive risk assessment on the topics of privacy and information security?

Votes Received: 794

A. Yes

21.2%

B. Yes, but there's more we should do in this area

41.8%

C. Not yet

37%

Source: PwC US Data Protection and Privacy webcast, "Tomorrow's Privacy - Balancing Commitments with Business Innovation“ (Feb 2012)

Privacy in the Headlines

The Sydney Morning Herald

National

Privacy commissioner investigates superannuation company CBUS

May 12, 2014

NEWS

Telstra fined after breaching privacy of 15,775 customers

Updated Tue 11 Mar 2014, 12:58pm AEDT

THE AGE

itpro

Revealed: serious flaws in myGov site exposed millions of Australians' private information

May 15, 2014 Comments 32

news.com.au

eBay urges customers to change passwords after massive cyberattack on databases; no PayPal breach

PREMIER OF VICTORIA Denis Napthine

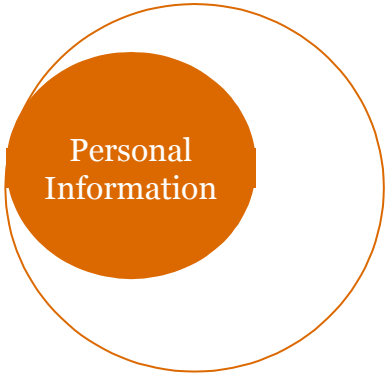
New framework for privacy and data protection and information sharing

Thursday, 12 June 2014

The Coalition Government today introduced legislation into Parliament to strengthen the protection of individuals' private information held by the Victorian public sector.

*What is covered by privacy?**

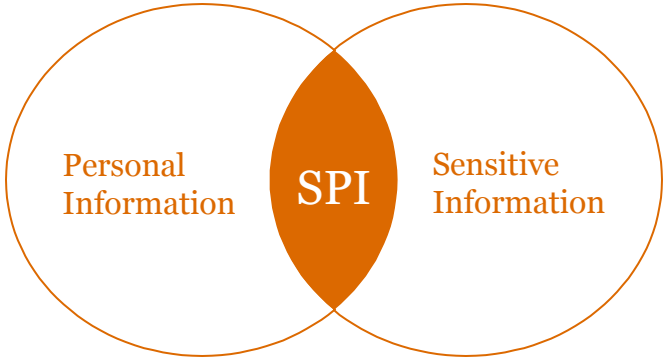
In Australia, privacy law generally relates to the protection of an **individual's personal information**. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.



Can it be attributed to an identified individual?

Examples include:

- *name, age, identification numbers, home or e-mail address, income or physical characteristics;*
- *opinions, evaluations, comments, social status, or disciplinary actions*
- *can include electronic, paper, voice or biometric information*



Sensitive personal information generally requires an extra level of protection

Examples include:

- *information on medical or health conditions;* ***[PHI]***
- *financial information;*
- *credit card information;* ***[PCI]***
- *racial or ethnic origin;*
- *political opinions;*
- *religious or philosophical beliefs;*
- *trade union membership;*
- *sexual preference; or*
- *information related to offences or criminal convictions.*

***Varies by country**

Privacy, security & confidentiality

Information lifecycle

Privacy - Personal information is **collected, used, retained, disclosed and disposed** of in conformity with the commitments in the organisation's privacy notice/policy and regulatory compliance.

Security – Protects the systems that hold the personal information against unauthorized access (both physical and logical) across the information lifecycle. Security is considered the technology enabler for privacy.

Confidentiality - Information designated as confidential is **protected as committed or agreed.**

Privacy risk… not just compliance

- Organisations face several financial risks associated with a breach:
  - Federal/state regulatory fines
  - Stock price decline
  - Remediation efforts

- Privacy/consumer trust as a market differentiator
- Negative impact to the brand
- Loss of employee, customer, & investor confidence

- Organisations are experiencing increasing lawsuits from:
  - Employees
  - Customers
  - Investors

•Enforcement actions from Australian and NSW Privacy Commissioner (Liz Coombs).

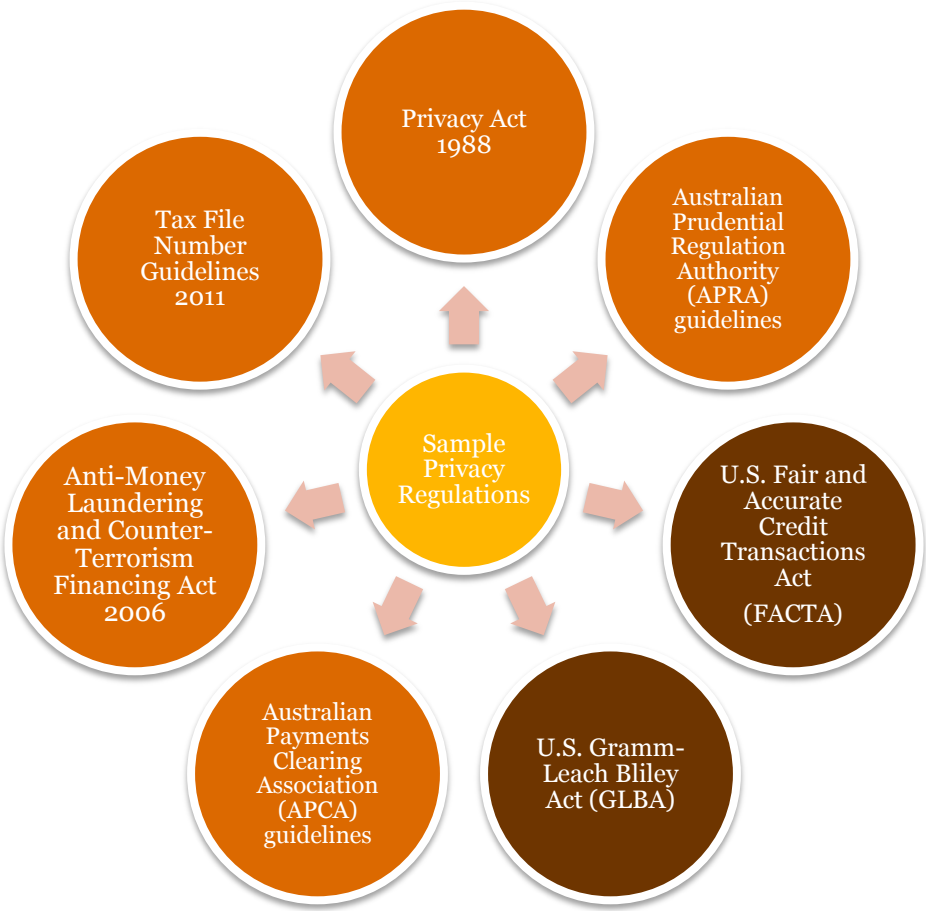
•Regulatory inquiries may require long-term third party remediation in order to verify regulatory compliance

No Single Legal Framework Exists Currently…

As such, our clients must comply with a combination of industry, sector and federal privacy laws based on:

- Types of business conducted
- Where business is conducted and where employees are located
- Where clients/customers are located

Let's consider a sample of privacy regulations that may apply for a financial services organisation…



The Privacy Act 1988 (Cth)

Key amendments were made to the Privacy Act to enhance privacy protection, which came into force in March 2014:

a. Introduced a **new single set of Australian Privacy Principles** (APP) for private and Commonwealth government entities
b. Implemented **more comprehensive credit reporting** provisions
c. Introduced a **revised regime for privacy codes and credit reporting codes**
d. Increased **the range of options for the Commissioner to encourage and monitor privacy compliance** and to resolve complaints
e. Introduced **civil penalties** for certain breaches of the Act.

Consider the Australian Privacy Principles (APPs)

The following are the 13 “Australian Privacy Principles” or APPs, as defined within the Privacy Act of Australia:

APP 1 — Open and transparent management of personal

APP 2 — Anonymity and pseudonymity

APP 3 — Collection of solicited personal information

APP 4 — Dealing with unsolicited personal information

APP 5 — Notification of the collection of personal information

APP 6 — Use or disclosure of personal information

APP 7 — Direct marketing

APP 8 — Cross-border disclosure of personal information

APP 9 — Adoption, use or disclosure of government related identifiers

APP 10 — Quality of personal information

APP 11 — Security of personal information

APP 12 — Access to personal information

APP 13 — Correction of personal information

Consider the NSW privacy legislation

- The Information and Privacy Commission NSW (IPC) oversees two laws that protect personal information and health information.
  - Privacy and Personal Information and Protection Act 1998 (PPIP Act)
  - Health Records Information Privacy Act 2002 (HRIP Act).
  - Other pieces of legislation have provisions affecting personal information and privacy, for example the Road Transport Act 2013.

- NSW public sector agencies are legally required to abide by the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) set forth in these state legislation to ensure individuals' privacy is protected.

Ensuring Privacy Compliance with Changing Operating Models

As Organisations Expand and Change Their Business/Operating Model…

What organisations are currently doing	Related privacy considerations
Expanding into new (global) markets	• What laws will I have to comply with? • Will information reside in one country or be transferred between several countries? • How should I protect any data I collect or transmit? • Do I need to have different policies for different customers based on geographic location? • How do I train and educate my employees to understand and comply with regulations for these new markets?
Off-shoring /Outsourcing certain business functions to third parties across a variety of countries	• Who is responsible for complying with local/national laws? • Will I need to comply with regulations enacted by the country my off-shoring partner is located in?
Expanding/Creating new products for customers	• Am I allowed to monitor consumers purchasing habits? • What data am I allowed to collect? • What data am I allowed to share with outside parties?

Questions Arise About Privacy and Protecting Sensitive Data…

What our clients are currently doing	Related privacy considerations
Targeting specific products to certain groups/sets of customers	• What data am I allowed to collect without consent to analyse customer behavior? • Are there restrictions on how I can use certain information? • How should I protect the data or customer information once I have it?
Providing excellent customer service based on personal attributes	• What data am I allowed collect? • Which data will I need to gain consent? • What are my processes to ensure that I can pass an audit?

The Internal Auditor's role

Triggers for Internal Audit's consideration

1	**Organisational Culture**	• What are the organisation's compliance requirements? • What is the culture of the organisation and what is the philosophy regarding data privacy and security? • Who will lead the efforts for information security & privacy (e.g., Steering Committee)? • How does the organisation ensure alignment between the management and staff? • What is the organisation trying to achieve with its information security/privacy program?
2	**Sensitive Information**	• What sensitive data does the organisation collect, use, disclose, dispose, etc.? • Is there a process to ensure customers are provided proper notice/choice/consent with respect to the organisation's data collection, use, and disclosure practices? • How does the organisation ensure data practices comply with customer privacy notices/policies? • Has the organisation classified and inventoried that data?
3	**Threats**	• Has the organisation's data been exposed – and would management know if it were? • Does the organisation know what breach indicators it should be monitoring? • Has the organisation released any new products that collect PII/SPI (i.e., websites, mobile apps, etc.)? • Has the organisation introduced any new technologies that access or store sensitive information (i.e., mobile devices , social media sites, cloud service providers, etc.)?
4	**Building Protections**	• Has the organisation established formal governance and controls around the data privacy lifecycle (i.e., notice, consent/choice, collection, access, disclosure, use, retention, disposal, security, etc.)? • Are such controls and safeguards periodically tested and monitored? • Have the controls and safeguards been updated to respond to changing business models?
5	**Responding to Incidents**	• Has the organisation established formal plans to respond to privacy and security incidents when they occur? • Is there a cross-functional team in place to monitor, investigate and respond to incidents? • Is the organisation prepared to respond to legal actions? • If a regulator were to inquire or investigate, would the organisation be prepared to respond?

Consider the Privacy Program Components

Considering your role in monitoring the Privacy Program

Internal Audit can play a role in the ongoing independent monitoring of a organisation's privacy program. Example monitoring activities include:

- Privacy program gap assessment
- Evaluation of, or assistance with, the organisation's periodic privacy risk assessment process
- Audits of compliance with established privacy policies and procedures
- Privacy training and awareness program audits
- Audits of any privacy related remediation or corrective action plans
- Audits of third party/vendor privacy practices

Consider your key stakeholders

The key stakeholders responsible for privacy can differ widely across organisations. Some of our typical stakeholders and issues are listed below:

Stakeholders	Scenario (examples)
Legal	• Regulatory complaints • Records Management
Marketing	• eCommerce initiatives • Customer relationship management • Social media campaigns
Information Security	• Audit findings • PCI readiness • Data breaches
Internal Audit	• Board or Audit Committee requests • Increasing the enterprise risk scope
Compliance	• Industry regulatory requirements • Regulatory examination
Privacy (if established)	• Governance structure • Operating privacy, how to "live" by the privacy policy

Key takeaways

Key Takeaways

- The privacy environment is getting more complex
- Understanding privacy expectations from stakeholders is key
- It's about risk, not just compliance
- Establish effective governance (by design) that starts at the top
- Follow the information that needs to be protected in your organisation
- Establish a formal, integrated program to monitor and audit privacy

Internal Audit should play a key role in sustaining and monitoring a tightly integrated enterprise wide privacy program

Additional questions?

Thank you for your participation

Andrew McPherson

Australian and East Cluster Internal Audit Leader

PwC

andrew.mcpherson@au.pwc.com

Direct: +61 (2) 8266 3275

Grace Guinto

Data Protection & Privacy – Capability leader

PwC

grace.guinto@au.pwc.com

+61 (3) 8603 1344