PRIVACY IMPACT ASSESSMENTS:

TOP TEN TIPS FOR ASSESSING PRIVACY RISKS

Nicole Hamacher, Privacy Impact Assessment Specialist, Treasury Board Secretariat

Eric Lawton, Senior Privacy Specialist, City of Toronto

Moderator: Renee Barrette, Director of Policy, Information and Privacy Commissioner of Ontario

2015 Ontario Connections Conference

Outline

You have been asked to do a Privacy Impact Assessment (PIA). Now what?

The focus of the presentation is on providing you with answers to the following questions:

- **What is a PIA?**
- **Why** do you need to do this?
- **When** is a PIA conducted?
- **Where** do you start?
- **Who** should conduct the PIA? Who needs to be involved?
- **How** do you identify privacy risks?
- **How** do you get buy-in? **How** long does this take?

What is a PIA?

- A PIA refers to a process/approach for identifying and analyzing privacy risks when changing or developing programs or systems." (OPS PIA Guide, page 5)
- A good PIA analysis provides senior management and program and system designers with sufficient information to reduce, mitigate or avoid different types of privacy risks.

Top Tip: A PIA is a point in time analysis.

Why do a PIA?

- **Ethical** – respond to Fair Information Practices and transparent personal information handling practices.
- **Risk mitigation** – the best tool to identify privacy risks, document countermeasures and implement mitigation strategies.
- **Compliance** – internal directives, policies and legal and legislative requirements
- **Save time and money** – avoid costly re-designs and risk of project cancellation.

Top Tip: Put yourself in the shoes of the data subject.

When to do a PIA?

- When a program/initiative/technology involves the personal information of an identifiable individual.
- Remember to choose the right tool because you may not need a full PIA to begin the process.

Top Tip: Begin the PIA at the earliest opportunity.

Who Should Conduct the PIA?

- While privacy professionals have the knowledge, skills and abilities to conduct PIAs, you may not have access to a dedicated PIA Specialist.
- PIA Reports can be conducted by a subject matter expert (e.g., policy, business, project member) by using publicly available guides and tools.

Top Tip: Do not do this alone!

Where should you start?

- Understand the project/program description and scope (e.g., what is happening, why and timelines)
  - Is personal information involved?
- Answer the question, “What information is being handled, by whom and why?”
  - Need to understand the data flows
  - A data model identifies the data elements and modality (e.g., one to many relationship) but doesn’t identify who is handling the information and for what purposes.

Top Tip: Begin with your data flow diagram.

Methodologies

There are many different methodologies that can be used including:

- Canadian Standards Association Fair Information Principles/Practices
- Privacy by Design foundational principles
- Test for Necessity and Proportionality
- Legislative compliance review

Top Tip: Take advantage of existing methodologies but do not cut and paste.

How do you identify privacy risks?

- Common privacy risks:
  - Unauthorized access/disclosure, identity theft, secondary uses without data subject's knowledge, inaccurate information, excessive retention, and transaction monitoring/big brother – real or perceived risks of unauthorized access and profiling
- Common privacy harms – loss of liberty, customer trust, discrimination, stigmatization, economic loss (e.g., due to identity theft)
- Once you identify the privacy impacts you need to identify mitigation strategies (how can we reduce the risk of those privacy impacts – what action(s) can we take).

Top Tip: Do not forget internal threats and ask yourself, "What is the worst thing that could happen?"

Identify Mitigation Strategies

- Work with the project team to design project or initiative in a way that mitigates the privacy risks or impacts.
- Mitigation strategies do not necessarily include strategies to eliminate risks.
- Identify actions that will reduce risks identified in your analysis.

Top Tip: Tailor workable solutions to the risk owner.

How do you get Buy-in (PIA signed)?

- Ensure that you understand the **risk tolerance** (what can be managed) and **risk appetite** (what is willing to be managed) of the responsible senior decision makers and that your PIA speaks to this
- Use the **project or risk owner's language**
  - Use terms found in mandates, business plans, public commitments, etc.
- **Rank/prioritize privacy risks and actions**
- Ensure that your PIA report **clearly communicates** the privacy risks and is shared with the senior decision makers responsible for the project or initiative.

Top Tip: Leverage the collaborative relationships with partners and understand risk owner's business plan.

How long does this take?

- "It depends"
- I've done all this work, I'm done, right?
  - PIA Report is a point in time assessment; new issues and changes impacting privacy may arise during the program/project
  - Align review of PIA Report/Mitigation Plan with existing review/approval processes: financial/budgetary cycles, strategic/operational planning review, etc.

Top Tip: Do not underestimate the time it takes to do the PIA, write the PIA report and for your partners to complete their review.

The Top Ten Tips

1. A PIA is a point in time analysis.
2. Put yourself in the shoes of the data subject.
3. Begin the PIA at the earliest opportunity.
4. Do not do this alone!
5. Begin with your data flow diagram.
6. Take advantage of existing methodologies but do not cut and paste.
7. Do not forget internal threats and ask yourself, “What is the worst thing that could happen?”
8. Tailor workable solutions to the risk owner.
9. Leverage the collaborative relationships with partners and understand risk owner’s business plan.
10. Do not underestimate the time it takes to do the PIA, write the PIA report and for your partners to complete their review.

Resources

1. OPS Privacy Impact Assessment Guides and Tools available through Information, Privacy and Archives Division, MGCS at web.foi.mgcs@ontario.ca
2. *Planning for Success: Privacy Impact Assessment Guide*; https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1502
3. *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*; https://www.ipc.on.ca/English/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=574

Resources (2)

4. Roger Clarke's PIA resources - http://www.rogerclarke.com/DV/
   - PIA: Its Origins and Development (2009)
   - Australian Privacy Foundation Policy Statement on PIAs
5. *Conducting Privacy Impact Assessments Code of Practice* (2014) and *Privacy Impact Assessment and Risk Management* (2013), UK Information Commissioner's Office - https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

Contact the IPC

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333/1-800-387-0073
TDD/TTY: 416-325-7539
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca