8 Pointers for Conducting a Privacy Impact Assessment

Safeguarding the privacy of confidential information whether it pertains to the organization or its individual employees, contractors, customers and clients, is an imperative. One key step is to conduct a so called Privacy Impact Assessment (PIA) to evaluate your current information systems, technology, programs and procedures to identify potential threats to privacy and then use the results of the evaluation to decide which measures to take to manage the risks you identify. Government agencies are required to conduct PIA; but PIAs also make sense for private sector organizations even if not required by legislation. And now the federal Privacy Commissioner has issued guidelines on how to conduct PIAs.

1. **Start Early**

You'll get the most bang from your PIA buck if you start the process early. If possible, begin at the outset of program development so you can address identified risks as part of basic program design and architecture.

2. **Define the Scope of Your PIA**

A common problem with PIAs, according to the Commission, is failing to clearly define its scope and parameters. The guidelines suggest that before you begin the PIA, you spell out what you are and are not assessing. Then make sure that these definitions are consistent with the data flow diagram included in your PIA report.

3. **Check the Privacy Commission Websites for Guidance**

The federal and many provincial privacy commissioners have published detailed guidance about doing PIAs and addressing the issues that your PIA will address, e.g., biometrics, cloud computing, mobile apps, covert and overt video surveillance.

4. **Consult with Stakeholders**

Consider how your program, product or initiative may impact others. Consulting with stakeholders both within and outside your organization can help ensure that all risks to privacy are identified. The privacy experts within your own organization are valuable partners, as they can provide you with advice and recommendations on privacy issues and national and international privacy standards to be considered.

5. **Address the Technicalities**

The Treasury Board Secretariat (TBS) and Communication Security Establishment (CSE) are among the government agencies that have created detailed standards and guidelines addressing the technical issues that arise when completing a PIA. For example, TBS' Operational Security Standard: Management of Information Technology Security (MITS) requires that a Threat and Risk Assessment (TRA) be conducted for every program, system or service.

6. **Submit the PIA to the Commissioner**

The TBS Directive on Privacy Impact Assessment requires covered institutions provide a copy of all PIAs to both the TBS and Privacy Commission.

7. **Implement the Plan**

Don't bother to undertake the PIA process unless you're prepared to implement the necessary mitigation measures identified in your PIA report. Make sure your report includes detailed action plans for proposed mitigation measures, including timelines, target completion dates and assignment of specific positions or persons responsible for implementation.

8. **Monitor Your PIA**

Treat the PIA as an ongoing process, not something you do just once. Once mitigation measures are in place, monitor them regularly to ensure they're effective and, if not, what changes or corrective measures are necessary.