Australian Government
Office of the Australian Information Commissioner

10 steps to undertaking a privacy impact assessment (PIA)

When developing or reviewing a project, consider the need for a privacy impact assessment (PIA). A PIA identifies how a project can have an impact on individuals' privacy, and makes recommendations for managing, minimising or eliminating privacy impacts. The Office of the Australian Information Commissioner (OAIC) recommends that organisations and agencies conduct PIAs as part of their risk management and planning processes.

Each project is different, but a PIA should generally include the following ten steps.

1. Threshold assessment

Ask if any personal information will be collected, stored, used or disclosed in the project. If the answer is yes, a PIA is usually necessary. Keep a record of this threshold assessment.

2. Plan

Plan the PIA. Consider: how detailed the PIA will be, who will conduct it, what is the timeframe, what is the budget, who will be consulted and how will the recommendations be implemented and monitored.

3. Describe the project

Prepare a project description to provide context for the PIA project. The project description should be brief, but sufficiently detailed to allow external stakeholders to understand the project. It should be written in plain English, avoiding overly technical language or jargon.

4. Identify and consult with stakeholders

Identify the project stakeholders. Consulting them can help to identify new privacy risks and concerns, understand known risks better, and develop strategies to mitigate all risks.

5. Map personal information flows

Describe and map the personal information flows in the project. The map should detail what information will be collected, used and disclosed, how it will be held and protected, and who will have access to it.

6. Privacy impact analysis and compliance check

Analyse how the project might impact upon privacy, both positively and negatively. Ask questions such as: Do individuals have to give up control of their personal information? How valuable would the information be to unauthorised users?

7. Privacy management — addressing risks

Consider options for removing, minimising or mitigating any privacy risks identified through the privacy impact analysis.

8. Recommendations

Make recommendations that identify avoidable impacts or risks and how they can be removed or reduced. Recommendations should include a timeframe for implementation.

9. Prepare the report

Prepare a report that sets out all the information gathered in steps 1 to 8. The report should be a practical document that can easily be interpreted and applied. The OAIC encourages the publication of PIA reports.

10. Respond and review

Monitor the implementation of the PIA report. A PIA should be an ongoing process that does not end with preparation of a report. It is important that action is taken to respond to the recommendations in the report, and to review and update the PIA.

Please refer to the OAIC's *Guide to undertaking a privacy impact assessment* available on the OAIC website: **www.oaic.gov.au**