

## What is a Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) is a structured process that helps an organisation to identify privacy and trust risks and to develop and implement strategies to address those identified risks.

A PIA is particularly effective when a new IT project which handles information about people is being developed and implemented but it can also be very useful to assess existing projects or services that customers are resisting.

A PIA can be conducted at the design phase, after completion of design, during the pilot phase, during all phases or even on a continuous basis to assess potential privacy impacts of a project.

## Why a PIA?

Increasingly organisations approach IIS for help because they are finding that compliance with privacy law is not enough to guarantee that their customers will be willing to accept a product or service provided through a new channel, such as the internet. Or the organisation may wish to develop more efficient business processes, but is worried that there may be brand damage or financial loss if individuals find the new process privacy intrusive. Others recognise the competitive edge to be gained from implementing privacy best practice.

Conducting a PIA to manage data privacy impacts actively and early is now becoming part of normal business practice.

## How do we do a PIA?

IIS conducts PIAs building on the process outlined in the Office of the Privacy Commissioner's (OPC) PIA guide. Key phases of this process include:

- **Information gathering** – The result of this phase is a description of the project and its information flows and the purpose of collection, use and disclosure of personal information in the project. This lays the foundation for analysis in the next stage of the project.
- **Analysis** – This phase assesses the project against privacy principles. In addition, IIS looks at other privacy risks that an organisation should address to better achieve consumer confidence and trust in the product, service or new process.
- **Consultation** – This phase enables an organisation to present information about a project to stakeholders on its own terms and to gain useful input at an early stage. Good consultation can generate a sense of ownership, trust and understanding amongst stakeholders.
- **Recommendations and report** – based on the analysis and input from consultation IIS provides practical recommendations in its PIA reports about how to allocate and mitigate individual privacy risks.

## The IIS Value Add

While the IIS PIA methodology builds on the OPC PIA Guide, it also incorporates into its analysis findings of new research into best practice privacy risk management about how to encourage *trust* from individuals.

Research is showing that whether individuals are prepared to trust a new technology or project often depends on the risks of failure of any sort and who bears that risk when it comes to pass.<sup>1</sup> The goal of the IIS approach is to create an electronic environment which inspires individual confidence, trust and willingness to engage.

To achieve this, when conducting its PIA analysis, IIS considers how an organisation can use four key tools to help build positive privacy solutions into its projects:

- **Law** – especially for public sector agencies, is the legal framework right? Does it properly promise enforceable protection?
- **Technology** (its design and implementation) – is technology being deployed in a way that enhances the protection of personal information and delivers organisational policy and legal obligations?
- **Governance** – what governance frameworks are in place to ensure that the promises of business process, technology platforms and legal obligations are actually being met?
- **Safety-Net** – what is in place that ensures when something goes wrong that individuals do not bear a disproportionate level of risk given that they are the party least able to manage, mitigate or bear it?

## IIS expertise and experience

Malcolm Crompton is well acquainted with PIAs and how to do them. In his role as Australian Privacy Commissioner (1999-2004), Malcolm Crompton initiated the development of the PIA Guide, since issued by the Office of the Privacy Commissioner, to help organisations conduct PIAs.

## Recent PIAs conducted by IIS

IIS has helped a number of organisations to build privacy into their projects through a PIA process including:

- A Smartcard and PKI authentication system for a major Australian financial institution
- A two factor authentication system for an international technology company
- An electronic health record project for a government agency in Australia
- A client records system for a government department in Australia.

<sup>1</sup> See "Trustguide Final Report", October 2006, UK DTI et al, online at [www.trustguide.org.uk](http://www.trustguide.org.uk)