EXECUTIVE BUY-IN FOR PRIVACY IMPACT ASSESSMENTS

Under the *Privacy and Data Protection Act 2014* (**PDP Act**), Victorian public sector organisations have an obligation to responsibly collect, handle and protect the personal information they hold.

One way to facilitate this is by undertaking privacy impact assessments (**PIA**). A PIA is a process that assists organisations in analysing a program’s impact on individuals’ information privacy, assessing compliance with relevant privacy laws, identifying potential privacy risks, and developing risk mitigation strategies.

Convincing people that PIAs are necessary and worth the time is easiest when your executive sponsors endorse the PIA process. Getting executive buy in for PIAs is vital for incorporating them into your organisation’s program planning processes.

However, privacy in general is often a low priority for the executive until an incident occurs and remediation is required. A PIA can be seen as a hurdle that costs time and resources; constrains the scope and impedes the progress of programs; or a compliance exercise that provides no tangible benefits. Some executives may not be aware of what a PIA process involves or the benefits of undertaking one.

This guide aims to assist privacy officers, project managers or other employees in overcoming these misconceptions and provides practical tips for obtaining executive support for the PIA process.

BENEFITS OF DOING A PRIVACY IMPACT ASSESSMENT

PIAs can have many benefits for individual programs and the organisation as a whole. Getting executive buy in will require you to sell the benefits of undertaking a PIA to your organisation’s executive..

Organisations

PIAs offer many benefits to organisations. A PIA:

* builds public trust and confidence in your organisation’s information handling practices, and develops your organisation’s social licence to use citizens’ personal information;
* improves your organisation’s information management practices, leading to better informed decision making and improved accountability and transparency;
* finds gaps in your organisation’s processes and practices, including ones unrelated to privacy;
* avoids costly mistakes that may have adverse financial and reputational impacts on your organisation;
* reduces potential future legal expenses and concern from the media or public by demonstrating your consideration of privacy issues;
* facilitates collaboration between different business units within your organisation;
* helps your organisation determine the appropriateness of engaging third parties by assessing their information handling practices and ability to comply with relevant privacy obligations; and
* assists in fulfilling your organisation’s obligations to uphold values such as transparency, impartiality, accountability and human rights, as mandated by the *Public Administration Act 2004*.

Programs

PIAs offer many benefits to programs. A PIA:

* helps ensure compliance with the PDP Act, and other relevant legislation, such as the *Victorian Charter of Human Rights and Responsibilities Act 2006*;
* demonstrates that your organisation has done its due diligence by considering privacy implications;
* identifies which individuals or teams should have responsibility for different aspects of the program, and identifies overlooked parties that could provide valuable input if consulted early;
* finds potential privacy and information handling issues with a program early – fixing issues retrospectively can be more expensive and time consuming;
* helps assess other elements of a program such as overall risk and security – the process of undertaking a PIA can flag other issues that go beyond privacy;
* minimises potential harms to individuals by identifying a program’s privacy risks and creating strategies to mitigate them;
* enhances the legitimacy of your program, especially where compromises or trade-offs to individuals’ privacy are necessary; and
* provides stakeholders with the opportunity to offer their perspectives, insights and concerns through consultations that may occur as part of the PIA process, resulting in a better-informed program.

TIPS FOR SELLING PRIVACY IMPACT ASSESSMENTS

When seeking support for conducting PIAs, frame PIAs as a planning tool – part of your project methodology – rather than a ‘tick the box’ compliance exercise. The PIA process will help you design your programs to enhance privacy and benefit your organisation. Also consider how PIAs can tie in with the objectives of your organisation.

PIAs are iterative processes – as programs evolve it is best practice to revisit your PIAs. Your program or organisation is not restricted by the initial process, and the resulting PIA template or report can be a useful reference point for future changes to the program.

Adopting PIAs does not have to be difficult. They can be incorporated into your organisation’s business as usual activities – they often fit neatly into existing assurance, risk management and policy development processes.

Different programs require different approaches, and some PIAs will be straightforward and easy to conduct, requiring minimal resources. Conversely, the PIA process may be more intensive where the program is complex; however, you do not necessarily have to conduct the PIA by yourself – there is always the option of enlisting outside expertise to assist you in undertaking the PIA process.

OVIC has a [PIA template and guide available](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/) to assist organisations in undertaking a PIA. While OVIC cannot conduct a PIA for you, we are happy to provide general feedback.

**Disclaimer:** The information in this document is general in nature and does not constitute legal advice.