Privacy Commissioner
Te Mana Mātāpono Matatapu

How to do a Privacy Impact Assessment

Contents

Overview

The basic steps in every PIA:

1. Gather all the information you need to do the PIA and sketch out how and where the information you intend to gather will go.
2. Check this against the information privacy principles (IPPs).
3. Identify any real privacy risks and how to mitigate them.
4. Produce a Privacy Impact Assessment report (use our report template to help).
5. Take action.
6. Review and adjust the PIA as necessary as the project develops.

See page 6 for a step-by-step guide on how to create a PIA.

Other steps that may be useful

Depending on the complexity of your project, you may need to add various other steps into your planning. These can include:

- Get an external view of your PIA.
- Consult with stakeholders.
- Establish better governance structures to manage personal information.
- Manage any risks by using third-party contractors.
- Align the PIA with the organisation's existing project-management methodologies.
- Publish your PIA.

For simple projects, the PIA process may be very quick, and the PIA may end up being only a couple of pages long. If your project is more complex, the resulting PIA may be long, detailed and highly technical – but if that's the tool you need to do the job successfully, then it's likely to be worth the investment.

There are several steps that need to be a feature of every thorough PIA. Then there are some other steps that may also be useful, depending on the size and complexity of your project.

Questions to answer before you start

When to do a PIA

A Privacy Impact Assessment isn't a last-minute legal compliance checklist – rather it's an active tool to help inform the major decisions involved in planning and implementing your project. Therefore, doing a PIA early in a project's life is going to be most useful.

The PIA will help you get the system and operation design right and avoid expensive and time-consuming pitfalls further down the road. Flushing out the potential issues at the conceptual stage of the project will show you what implementation details you're going to need to address. It will help you craft a more accurate project plan, as well as providing greater assurance that the project will be successful.

Build checkpoints into your project plan

Inevitably, projects change during their lifetime. You may not be able to answer every question in an early PIA – more information may come to light later. This is normal.

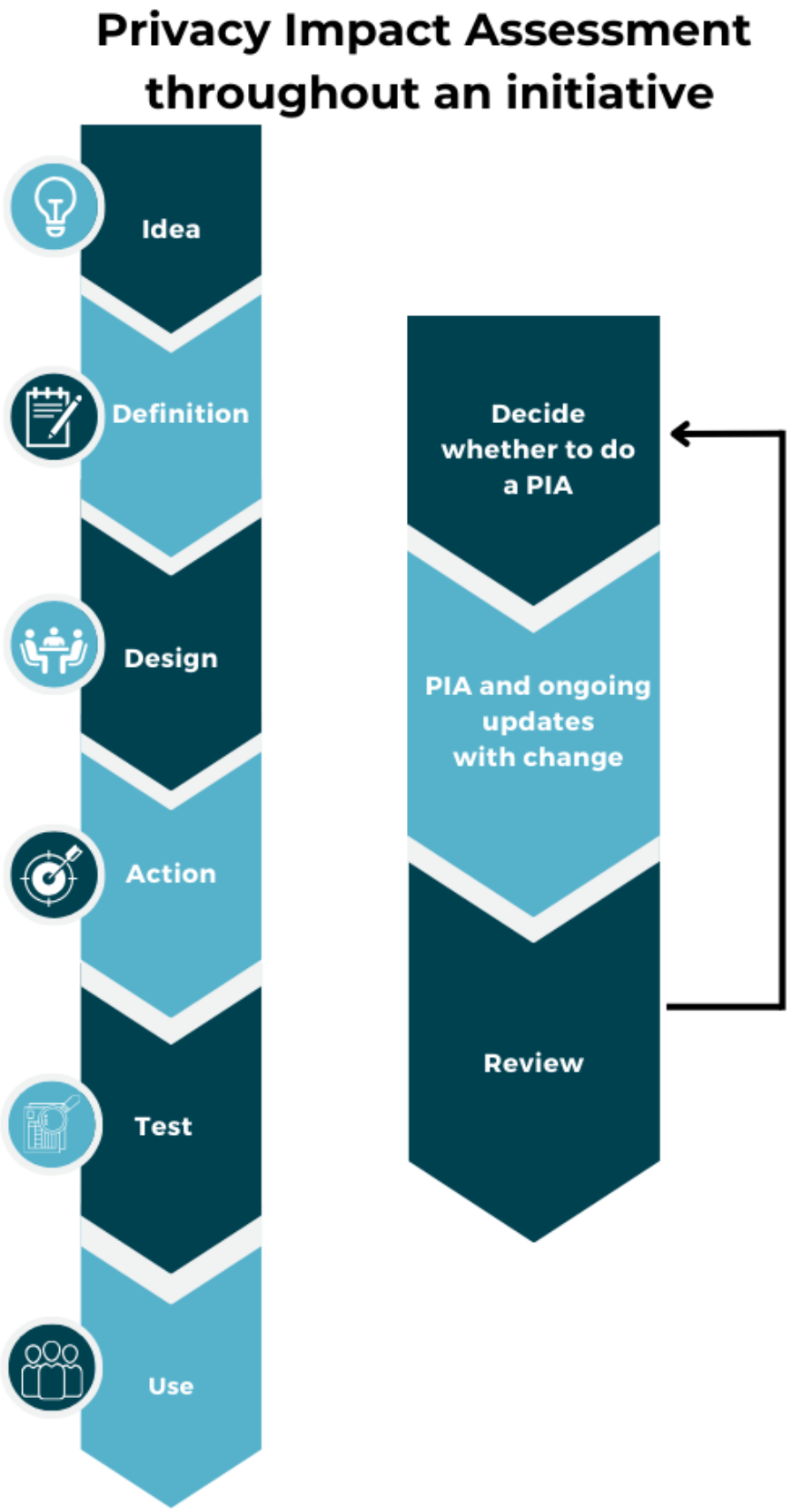
To manage this, build one or more PIA checkpoints into your project plan, where you'll ask whether anything significant has changed since you did the PIA. If it has, then slot that information into a new version of the PIA and go back through the steps to check that there are no new privacy risks or, if there are, that the new risks are clearly identified and managed.

Example

A PIA as part of the design of a new IT system

If your project is a new IT system that collects, stores or processes personal information, it will be risky to put off doing a Privacy Impact Assessment until after you've tendered for and designed the system. The PIA will help you design the system to manage that personal information well. You'll find it much harder and a lot more expensive to redesign or rebuild the system later to address any risks that the PIA exposes.

This diagram shows how a PIA fits into the life of a project.



Who do I need to talk to?

Most of the people you will need to engage with are internal stakeholders. However, there may be some external stakeholders you also need to talk to.

Make sure you're aware of who has the information you need, and when they're going to be available.

If you're a small organisation, there will only be a few people in the organisation you'll need to look to – the information might even all sit on one person's desk. In these cases, think about whether there are people outside your organisation who you can get some advice from – for example, business colleagues, the local Chamber of Commerce, or the Privacy Commissioner's website.

People who might need to be involved:

- People who are familiar with privacy, particularly the organisation's privacy officer.
- People who deal with security in your organisation – they're likely to be familiar with what you're trying to achieve.
- Business analysts and other project staff who will understand the business aims, what's being put in place, and when various steps need to be taken.
- IT advisers who'll be able to provide information on the systems being used, how the personal information will flow through the system (including how it will be stored and processed), and whether there are any security implications.
- Marketing and communications advisers who will help in understanding how the organisation uses information and can help coordinate any consultation needed for the PIA.
- Risk and assurance people who can help you identify risks, controls, and other actions.
- Specialist staff groups who are affected by any proposals for handling personal information, such as call centre staff, information management staff, or human resources – they can give you the best information about how things will work on the ground.
- Customer or consumer groups.

Who should do the PIA?

You don't need to be a privacy specialist to put together a straightforward PIA. It doesn't have to be done by your organisation's privacy officer, or a lawyer. However, it's useful if the project team includes someone who is reasonably familiar with privacy and able to advise you about the privacy principles and the potential privacy impacts of the project.

If the PIA will be particularly complex, or particularly central to the success of the project, it's worth thinking about hiring an external expert.

Do I need to involve the Privacy Commissioner?

If your project involves:

- policy proposals or draft legislation that affects personal information or individual privacy
- an authorised information-sharing or information-matching programme
- or if a statute says the Privacy Commissioner must be involved

then the lead government agency is required to consult us.

The Cabinet Manual[1] requires government agencies to consult with the Privacy Commissioner when putting forward policy proposals or draft legislation that affects personal information.

Part 7 Subpart 1 of the Privacy Act (approved information-sharing agreements) and Part 7 Subpart 4 (authorised information-matching programmes) specify when and how the Privacy Commissioner must be consulted.

[1] At paragraphs 5.19, 7.68, 8.6, 8.72--78 and 8.86-89of the Cabinet Manual.

A step-by-step guide to completing a PIA

It's about covering all the bases – not the order of the steps.

As you work through the key PIA steps we discuss in this section, remember that it's the content of each step that matters – not the order you do them in.

So don't be concerned if you find yourself doing things in a slightly different order from how we've set out the steps below.

1. Gather all the information you need

The information you put together when you were deciding whether to do the PIA will be a good start for doing the PIA itself. Now is the time to gather all the details about what personal information the proposal involves and what is going to happen to it.

The key tasks here are:

- Describe the project – focus on what happens with personal information.
- Describe the personal information involved and what will happen with it.
- Describe the organisational context.

As you complete each of those tasks, add the information to a draft Privacy impact assessment report. You can use our "Privacy impact assessment report" template on our website as the basis for the report (adjust it as necessary to fit your organisation and project).

You can use the report either as a briefing document for managers or other decision-makers, or – if the decision is your own – as a record of what you decided to do and why.

Describe the project – especially the purpose of changing what happens with personal information

A PIA is a tool to help you achieve the aims of your project or your organisation more generally while also protecting personal information. There is often more than one way of designing a project to accomplish what is intended – a PIA will help to identify the least intrusive way of achieving that aim.

A major key to success is having a clear understanding of what the change is aiming to achieve, and how it will support your organisation's work.

Key points to cover

- Describe the project briefly.
- Describe the purpose of changing what happens with personal information – what is the business aim in making the change?
- Is the project a one-off activity, or does it involve a change to your ongoing information-management systems?

Describe the personal information involved and what will happen with it

The focus of any PIA is the personal information involved in the project and the positive or negative effects that the project may have on the privacy of the individuals affected by it.

It's important to think about the whole lifecycle of the personal information. For instance, the PIA will need to consider how that information is going to be stored, who's going to use it and why, how it's going to be kept up to date, how long it will be kept for, and what will happen if the individual whose information it is asks to see it. Without considering the whole lifecycle of the information, you won't be able to spot where the problems or the opportunities occur.

You'll also need to consider a broader range of information-management questions if, for example, your project involves sharing information with another organisation so that the individuals can receive a service more efficiently. You'll need to consider whether the sharing of information will take the individual by surprise – perhaps because it's different from what they were told when you collected the information from them? If so, will you need to tell them what's going on? Also, how will you make sure the information is kept secure when it's being sent to the other agency, and that it won't be accessible to people who could misuse it?

Describe the flow of personal information through its lifecycle in your organisation

Key questions to answer:

- What personal information is currently collected and used? How does it flow through your organisation's systems?
- How will your project change the information flow?
- Describe all the changes to personal information involved in the project. For instance:
  - Is new personal information being collected? If so, where is it coming from?
  - If the project involves information your organisation already holds, will you be using the information for a different purpose? If so, why, and how?
  - What measures are in place to ensure the information is accurate and up to date?
  - Will your organisation tell the individuals what's happening to their information? If so, how will it tell them?
  - Who will have access to the information inside your organisation? Who will have access to it outside the organisation?
  - How long will the information be kept for? How will it be disposed of?

Using information flow diagrams

There are many ways in which you can set out the lifecycle of personal information. However, an information flow diagram – or a series of diagrams – can be a particularly clear and simple way of showing exactly where personal information is coming from, where it's going, how it's going to be used, and who it's going to be used by (see example above). This can help you identify measures that can improve information security and reduce privacy risks.

Describe the organisational context

It's important to consider privacy implications in the context of the project, and in light of how your organisation works – particularly its existing approach to handling personal information. For example, you'll need to know whether any risk mitigation or other change that you recommend for the project is likely to be workable in the context of the entire organisation.

Considering the organisational context will also help you to be aware of the likely downstream effect of the project in your organisation and enable you to predict and address potential privacy risks. For example, if your project involves one division of your organisation collecting a new piece of personal information for a particular purpose, how long will it be before another division decides they could use it too? Anticipating this kind of potential "scope creep" is an important part of any PIA.

Types of background information to include

Bring together the necessary background information about your project and organisation. This might include:

Governance, management and roles and responsibilities describing privacy in your organisation (your privacy officer or legal team should be able to help you with this).

- Policies, standards, and procedures relating to personal information (such as privacy statements, and retention or security policies).
- How privacy fits in with risk management in your organisation (for example, does your risk management framework consider risks to the people whose information you hold, rather than just risks to the organisation?)
- Overall processes and controls that affect privacy, such as disposal processes.
- Security controls, such as how access to your information systems is managed.
- Training and awareness programmes on privacy and security.
- Monitoring and auditing of any incidents that occur, and how these are dealt with.

2. Check against the privacy principles

As well as providing the legal framework that your organisation will need to comply with, the principles in the Privacy Act also provide a useful practical checklist for handling personal information properly throughout its entire lifecycle. This includes:

- collecting the information
- storing it and keeping it secure
- checking the accuracy of the information
- letting people have access to it so they can see what you know about them
- using or disclosing the information
- destroying the information.

The next section contains a summary of the privacy principles and information about the risks and mitigations to help you complete your PIA. The full text of the principles is section 22 of the Privacy Act. More detailed advice about what the privacy principles entail is available on our website privacy.org.nz.

Consider the personal information involved in the project and how the privacy principles apply.

Key points to cover

For each privacy principle:

- Is it relevant? (if not, simply note that it is not relevant and why).
- Identify the personal information that is relevant to that principle.
- Is the change consistent with the privacy principle? If so, how? Or will it enhance compliance?.
- Does the change create more risks of harm to the individual? If so, how might it adversely affect the individual? Or does the change eliminate risks in the existing system?

Example

A new mobile app

A business develops a mobile app that will collect various items of information about users, including information about their location. Questions the company will need to ask about that location information include:

- Why is it necessary to collect information about location? Is it a "need to know" or just a "nice to have"?
- What exactly will the business use the location information for?
- Will anyone else have access to the information?
- Will it be shared with third-party providers to run ads in the app, for instance?
- How will users know the information is being collected and why?
- What will happen if users don't agree to provide the information? Do they have to consent to download the app? If so, is this reasonable? Can the user opt out (even if at the cost of some of the functionality)?
- Can the user change their mind and opt out of sharing location later? What will happen to the information the agency has collected if they do so?
- Is the user specifically and clearly asked for permission? How clear is the privacy statement?
- How long is user location information kept for? Is it aggregated, or linked to the user by information obtained from elsewhere or from the user?
- How is the information going to be protected against misuse and loss?

It's important that the PIA take a critical and impartial approach to these types of questions, as they will drive the design choices the business makes. It's easy to get enthusiastic about the business opportunities resulting from collecting and using personal information, but consideration of how the individual concerned could be affected leads to better design in the long run – and a greater chance that the product will succeed.

3. Identify any privacy risks and how to mitigate them

Ideally, a PIA will identify both risks for the individual, and opportunities to benefit the organisation by protecting privacy better. While this section focuses on identifying and mitigating risks, you could use a similar analysis to identify and maximise opportunities.

What is a privacy risk?

A "privacy risk" is the risk that a proposal will fail to meet individuals' reasonable expectations of privacy – for instance because it breaches the Privacy Act, or unreasonably intrudes into their personal space and personal affairs or runs contrary to what your relationship with your clients suggests should happen.

Calculating risk is not simply about assessing whether the project will be legally compliant. It's possible to comply with the law and for the behaviour still to affect whether your clients' reasonable privacy expectations are met. The nature of your relationship with them may suggest that you should give even better protection than the law requires. The privacy principles provide a good framework for asking yourself the right questions – both legal and non-legal – about the impact on your clients.

Risks to an individual will often directly equate to risks for your organisation. Privacy breaches will have a direct impact on the organisation's reputation, and loss of trust can make it harder and more expensive to meet the aims of the project.

Consider not only the direct risks from the proposal, but also any knock-on effects. If you take too narrow a lens, you may miss an important, wider effect on the individuals you deal with.

How far do I have to go?

A PIA doesn't set out to identify and eliminate every possible risk to an individual from using their personal information or impacting on their privacy. However, it should:

- identify any genuine risks to the individual (that is, risks that aren't unrealistically remote or trivial)
- assess how serious those risks are.

Next:

- identify how to mitigate serious or medium-level risks
- determine your organisation's attitude to risk in the context of this project. Sometimes an agency may have a very low tolerance to risk – for instance where its relationships with its customers or clients are so important that it can't afford even relatively minor risks to eventuate.
- identify any serious or medium-level risks that the organisation decides it is not going to mitigate.

How to identify the risks

If your organisation is large, there may also be a specialist team (perhaps Risk and Assurance, Internal Audit, or Corporate Compliance) that can help you with how the organisation generally approaches the issue of identifying and managing risk. There may well be a specific format that it is best for you to use.

For organisations without specialist risk frameworks, we have provided a template for a risk and mitigation.

Populate your risk table with the risks you already know about from step 2 and identify the likely impact on the individuals. You can then use that as a basis for a more thorough analysis. Make sure you talk to other people involved in the project or get a view from an external person who may be able to see risks that you have missed. Other possible steps, depending on your project, could be:

- a workshop including the key people involved
- a further desk-top review of documentation
- interviews with key people involved.

Common examples of mitigations include:

- minimising the amount of personal information collected
- better and clearer communication with the individuals
- allowing individuals to opt in instead or making it easy to opt out
- designing the system to provide better security
- providing training and support for staff to help them get it right.

Try to ensure that your mitigation solution is practical and sustainable. Reviewing the project once it's operating will help to identify whether the mitigations are actually working as you've planned.

The following page has an example of how a few lines on this risk table might look, using the earlier example of a mobile app:

Reference number	R-001	R-002
Aspects of information assessed	What information the app collects	Third party providing advertising through the app needs access to information (age, gender)
Description of the risk	The app will collect more information than specified in the privacy statement	Third parties may misuse this information for their own purposes (spamming, hacking, etc)
Rationale and consequences for the agency or individual	The app will have greater functionality and lead to increased monetisation, but app users may object to collection beyond the current privacy statement	Data is never truly de-identified so may be misused exposing individuals to unexpected impacts. Individuals distrust unexpected disclosures to third parties. Third party access to user information is a source of revenue.
Existing controls that contribute to manage risks identified	The business has a clear purpose for collecting the personal information (but app policy does not currently reflect it)	De-identify data as much as possible. Contract with third party also specifies what can and can't be done with information
Assessment of residual current risk	Medium/possible Moderate harm	Medium/possible Moderate harm
Recommended additional action reduce or mitigate risk	Put a process in place to manage clear notification and consent for additional collection by the app in line with the new purpose	Extend contract with third party to disallow re-identification or reuse of data for different purposes
Residual risk remaining despite new safeguards	Low/unlikely Minimal harm	Low/unlikely Minimal harm

Reference number	R-003	R-004
Aspects of information assessed	To function the app requires a persistent account, tied to an individual	Username and password are collected by the app
Description of the risk	Behavioural information is collected over time, in addition to personal information collected at download/ registration	Some users use one password across multiple accounts, which could reduce the security of the system elsewhere
Rationale and consequences for the agency or individual	There is an administrative need, as the app won't work without a persistent account. But app users might object to more behavioural information being collected, and might abandon it for this reason	Hard to prevent people from recycling passwords. If an external account is compromised, all other accounts using the same username and password are vulnerable, including the app
Existing controls that contribute to manage risks identified	Privacy notice clearly outlines what information can be used for (e.g. account persistence, and customer service – which covers targeted advertising)	Credential information is encrypted; process to change/reset passwords is secure; hashed passwords are salted, but this won't prevent use
Assessment of residual current risk	Low/unlikely Minimal harm People often do not read the privacy policy – system design should still protect them as much as possible	Medium/possible Moderate harm
Recommended additional action reduce or mitigate risk	Amend retention policy to ensure that app user logs are deleted when they are no longer needed (easy additional protection)	Require users to create a unique password for the app, changed regularly, using criteria unlikely to have been demanded by other accounts
Residual risk remaining despite new safeguards	Low/unlikely Minimal harm	Low/unlikely Minimal harm

4. Produce a PIA

The PIA is a major reference point for you and for your organisation. It should at least:

- include all relevant information about the project and what it is intended to achieve
- describe how information flows through the system
- include analysis against the privacy principles and other relevant material to show what the privacy impacts are (both positive and negative)
- identify key risks and how to mitigate any negative impacts
- recommend any necessary changes
- identify whether the PIA should be reviewed during the project, and/or once the new system is operating.

5. Take action

There's little point investing even modest amounts of time or resources in a PIA and then failing to take action. An action list can help you track and manage the decisions you take because of the PIA.

The action list may contain items to be completed as part of the project itself, or it can be integrated into normal operations (such as maintaining a risk register, or as part of a security action plan).

Make sure that the action list clearly identifies who's responsible for doing what. Also make sure that it notes any relevant timelines and contingencies (for example, Action A needs to be completed by date B so that Stage C of the project can start).

In large or complex projects, there might be several versions of a PIA. It's important that any actions or recommendations from each update of the PIA are considered throughout the project. This may require designating someone in the project to take ownership of the action plan and report on progress, either within the project or within the organisation's existing governance framework.

The PIA may identify wider opportunities for action, so you can make privacy-enhancing changes throughout your organisation. For instance, it may show that there are other parts of your business where you might also achieve better security, better accuracy of information, and more effective business processes for managing personal information. If you spot an opportunity, take it – it's likely to make your business better.

6. Review the PIA and use it as a checkpoint once things are in operation

Projects are rarely static. Even small projects can morph as they progress. A PIA that was produced early in a project's lifecycle is unlikely to reflect the current state of a project.

Use your Step 4 report and your Step 5 action plan as a baseline for considering the project as it progresses. If there have been changes that have an impact on privacy, do quick updates of the report and action plan that record:

- what's changed
- what the new impact is
- how to address any new risk (or take advantage of any new opportunity).

This will ensure your PIA continues to be used as a tool to check that the project does what it is meant to do.

Once the changes are up and running, it is also worth using the PIA as a checkpoint for how the new process is operating. Is it working as anticipated, or are problems starting to emerge and further changes needed?

Again, using the PIA as a reference point can save you time and trouble.

Other steps that may be useful

Get an external view of your PIA

If your project is a substantial one, or the potential impacts on privacy are particularly significant, it will be worthwhile getting someone outside your organisation to check your PIA. They may identify something you've missed. They may have a better idea of how people who are not close to the project may react to what your organisation is doing – particularly the individuals who will be affected by the project.

Examples of people who can give you an external view might be:

- colleagues within your industry
- an industry association, Chamber of Commerce or representative group
- Office of the Privacy Commissioner
- a lawyer or a specialist in privacy law or information management
- IT specialists, systems architects, security consultant and so on.

Consult with stakeholders

Some projects will benefit from very wide consultation with stakeholders, both inside the organisation and externally. In particular, some projects will benefit from consultation with the individuals whose information you are using, or who will be affected by your project.

As part of your initial analysis, or your information-gathering exercise, consider who will have the best information to contribute or who might best flush out the risks posed by the project. If the answer is that your customers, or your staff, or external stakeholders might give you valuable information that you can't get elsewhere, then think about consulting with them.

Identify:

- who can give you the information?
- when consultation is needed and how long it will take (so that you have the information in time to use it)
- how far you need to go for it to be useful
- what you will ask them?
- what method you will use to get information from them (for example, a targeted survey, an email request to an external agency, or an online opportunity to respond).

Establish better governance structures for managing personal information

Protecting privacy is an ongoing responsibility, not something that your organisation should only consider as part of a change process.

Writing a PIA might be the first time your organisation has had to think about privacy issues. If so, use it as an opportunity to get people thinking about how to manage privacy better across the organisation.

In particular, make sure someone in the organisation is tagged with responsibility for managing privacy. Ensure privacy is one issue that's considered at the top table – solid leadership will make it far more likely that the organisation will get privacy right.

Manage any risks with using third-party contractors

If your project involves passing personal information to third-party contractors, this is a good opportunity to consider how to manage wider privacy issues relating to third parties who may have different standards from your organisation.

Questions to ask include:

- What privacy standards will you be holding the contractors to?
- Are they capable of meeting your expectations?
- How will you know whether they are competent?
- How will you know if something goes wrong?

You may be able to rework your standard contracts, or other documentation, so that it makes it easier and quicker to think about these issues when you engage a third-party contractor to do work for you in future.

Align the PIA with the organisation's existing project-management methodologies

Large organisations tend to have in-house project management tools. It's important for the PIA to fit with the way your organisation usually does things so that it has the best possible chance of being integrated into your business systems and of being effective.

For instance, for very large projects, or projects using "Agile", or Agile-like methodologies, approaching a PIA as a series of linked assessments may help the PIA and the principal project align better.

Publish your PIA

One of the benefits of doing a PIA is that it can increase the trust people have in your organisation and their willingness to work with you. If they're aware of what you've done to manage privacy, they may have more confidence in you. Publishing the PIA demonstrates that you take privacy issues seriously and that you do your best to manage them. If you're a small firm, for instance, publishing your PIAs may demonstrate that you're a cut above your competitors.

Public-sector agencies should seriously consider publishing their PIAs to demonstrate accountability, and as a proactive release of official information.

Of course, a PIA may need to be reworked to protect interests such as commercial confidentiality, client privacy, security of information or legal privilege. Publication is not an "all or nothing" exercise – it is better to take out certain elements of the report and publish the rest, rather than not publishing at all.