# Part 2 Appendix B:Template – Risk and Mitigation Table

This risk and mitigation table aims to help you to identify, describe and manage potential privacy risks involved in your project.

### Prioritising risks

A risk and mitigation table helps you to prioritise risks according to how likely it is that threats to privacy will materialise, and to gauge the severity of their potential impacts. You can then decide which controls are most needed.

This exercise will help you sort out what you should do now, what you should do soon, and what you could do later if resources allow it.

### Identifying safeguards

You may be able to identify areas in which adding privacy safeguards will help your project or organisation to function more efficiently and win greater trust from your clients. The appropriate use of privacy-enhancing tools and technologies may help to reduce the potential adverse effects of your initiative on privacy in a number of ways, and may reduce or eliminate the need for other safeguards.

***See some common examples of privacy risks in Appendix C***

## How this table is organised

This risk/mitigation table uses the **privacy principles** in the Privacy Act as a framework for working through the whole lifecycle of the personal information. Listing the risks you have identified in an orderly way, principle by principle, helps you make sure you’ve covered all the bases.

The table includes **eight different categories**:

* **Reference number:** Listing each risk with a separate reference number lets you record separate decisions about separate matters, and it will translate readily into your action plan. It also provides a useful short-hand reference for this particular risk in other supporting paperwork or discussions. Proposed safeguards and mitigations can also be numbered for ease of reference later on.
* **Aspects of information management**: identify each separate information-management aspect or phase that the project involves (such as collection, retention and disclosure)
* **Description of risk**: Identify each vulnerability (in the project’s current design) relating to that aspect of information-management – for example, new information requirements, system design needs that underpin the initiative, or other design decisions that could upset the project if not properly addressed
* **Rationale and consequences**: Why do these things matter – how could individuals or the agency be harmed? Also note where there are benefits that you want to maximise or ensure are maintained
* **Existing controls**: What current safeguards will help to minimise or manage the risks identified?
* **Residual current risk**: If the system is unchanged, what is the level of the risk?
* **Recommended mitigations or enhancements**: What additional measures can be used to remove, manage or mitigate the residual risk, or to enhance privacy safeguards?
* **Residual risk remaining**: What risk will remain even if new safeguards are put in place?

## Adapt this template to your needs

Adapt this risk mitigation template to suit your own purposes. You can use the template in a variety of ways. You can either include it in the PIA report, or you can cut and paste information from it to suit your own report style. It can double as a “privacy risk register” for your project, which you can then refer to as the project develops. You can produce new versions as proposals develop over time.

You may also wish to include a summary of each column of the table as an introduction for people reading your risk and mitigation table, to help them understand the different components.

|  |
| --- |
| **Assessment of potential risks and possible mitigations** |
| **Principle 1 : Purpose of collection of personal information** |
| Ref. no. | Purpose of collecting the information | Description of the risk  | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual current risk  | Recommended mitigations or privacy enhancements | Residual risk remaining despite new safeguards  |
|  | *Identify each aspect of the project that raises privacy issues*  | *Describe any vulnerability and the risk identified (that is, that could upset the project) noting any relevant legal rules and system design needs* | *Explain why this is an issue; the potential adverse impact on individuals (or the agency) and the benefit that you wish to continue to achieve* | *Document the systems and safeguards currently in place that act to minimise these identified risks* | *Assess the likelihood of the risk eventuating (high, medium or low) and how severe the harm would be with no new protections (serious to minimal)* | *Include recommendations for how these residual risks can be removed, managed, or mitigated, or further privacy safeguards to ensure the individual is protected* | *Detail any remaining vulnerabilities in the design that need to be managed.**Note risk level (high, medium or low) and the likely severity of harm without any new safeguards.* |

|  |
| --- |
| ***EXAMPLE ONLY - See “How to do a PIA” for more information*** |
| Ref. no. | Purpose of collecting the information | Description of the risk  | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual current risk  | Recommended mitigations or privacy enhancements | Residual risk remaining despite new safeguards  |
| R-001 | What personal information the app collects | The app will collect more information than is specified in the privacy statement  | App will have greater functionality and lead to increased monetisation, but app users may object to collection beyond current privacy policy and collection may breach law | Business has a clear purpose for collecting the further personal information but app policy does not currently reflect it | **Medium/Moderate**  | Put in place a process to manage clear notification and consent for greater collection by app once purposes change | **Low / Minimal** Some existing customers may still not realise the change has occurred  |

Privacy Impact Assessment – Risk and Mitigation Table

[*Insert a PROJECT TITLE or description of your project or proposal here*]

Note: See Appendix C, “Privacy Risks and Mitigations – Examples”

|  |
| --- |
| **Assessment of potential risks and possible mitigations to reduce or manage adverse effects** |
| **Principle 1 : Purpose of collection of personal information** |
| Ref. no. | Purpose of collecting the information | Description of the risk  | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual current risk  | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |
| **Principle 2: Source of personal information** |
| Ref. no. | Source of personal information | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual current risk | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |
| **Principle 3: Collection of personal information from the subject** |
| Ref. no. | Telling the individual what you’re doing | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual current risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |
| **Principle 4: Manner of collection of personal information** |
| Ref. no. | How you are collecting personal information | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual (current) risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |
| **Principle 5: Storage and Security of personal information** |
| Ref. no. | How you are storing and securing personal information | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual (current) risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |

|  |
| --- |
| **Principles 6 and 7: Access to and correction of information** |
| Ref. no. | Responding to people’s requests for information about themselves, or requests to correct information about themselves | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual (current) risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |
| **Principle 8: Accuracy etc. of personal information to be checked before use** |
| Ref. no. | What steps do you take to check the accuracy, relevance etc of personal information before you use it? | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual (current) risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |

|  |
| --- |
| **Principle 9: Agency not to keep personal information for longer than necessary** |
| Ref. no. | How long do you keep personal information and why? | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual (current) risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |
| **Principle 10: Use of information** |
| Ref. no. | What are you going to use the personal information for?  | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual (current) risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |
| **Principle 11: Disclosure of information** |
| Ref. no. | Who are you going to disclose the personal information to (if anyone) and why? | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual (current) risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |
| **Principle 12: Use of Unique Identifiers** |
| Ref. no. | Why do you need a unique identifier, and are you allowed to use this one? | Description of the risk identified | Rationale and consequences for the agency or individual  | Existing controls that contribute to manage risks identified | Assessment of residual (current) risk recognising current measures | Recommended additional actions to reduce or mitigate risk | Residual risk remaining despite new safeguards  |
|  |  |  |  |  |  |  |  |