



**Australian Government**  
**Office of the Australian  
Information Commissioner**

# Interactive PMP Explained

How to use the OAIC's  
Interactive Privacy  
Management Plan tool

[oaic.gov.au](http://oaic.gov.au)

**OAIC**

**July 2018**

# Contents

Key points .....	3
Introduction.....	3
What is a Privacy Management Plan (PMP)? .....	3
What is the Interactive PMP? .....	4
Measuring maturity.....	4
Interactive PMP: An overview .....	4
How do I access the Interactive PMP? .....	5
Is it compulsory to use the Interactive PMP? .....	5
When to use the Interactive PMP .....	5
Who should complete the PMP? .....	6
Who should measure and document agency performance against the PMP? .....	6
Sharing your agency's PMP and working with other agencies .....	7
Completing the Interactive PMP.....	8
Background .....	8
Step 1: Measure maturity.....	11
Step 2: Set your agency's actions.....	15
Step 3: Measure and document your agency's performance.....	16
Case study: Department of Workforce Planning .....	17
Completing the Interactive PMP for DWP .....	18
Additional actions.....	23
Appendix 1: Privacy Program Maturity Assessment Framework .....	24
Overview.....	24
Maturity assessment — key concepts .....	24
Detailed maturity descriptors .....	26

## Key points

- This guide has been developed to help agencies navigate the [OAIC's Interactive Privacy Management Plan \(XLSM 588KB\)](#) (**Interactive PMP**) and the accompanying Privacy Program Maturity Assessment Framework (**Maturity Framework**).
- Agencies are required under the [Privacy \(Australian Government Agencies — Governance\) APP Code 2017](#) (**Code**) to have a privacy management plan (PMP) which identifies specific, measurable privacy goals and targets and sets out how the agency will meet its compliance obligations under APP 1.2 of the [Privacy Act 1988](#) (**Privacy Act**). Under the Code, agencies must also measure and document their performance against their PMP at least annually.
- It is not compulsory to use the Interactive PMP to meet these obligations. However, the Interactive PMP is a tool which will assist agencies to meet these obligations in a simple, comprehensive and consistent way.
- The Interactive PMP will also help agencies to set realistic plans to lift their privacy maturity beyond their compliance requirements. Agencies can use the Interactive PMP to identify privacy goals that are realistic, relevant and that will deliver the most value to them.

## Introduction

This document provides important background information about the Interactive PMP, including an illustrated, step-by-step guide to creating and maintaining your agency's PMP. Note that APP entities that are not agencies may also use the Interactive PMP and related materials to assist with developing their PMPs.

Before using the Interactive PMP to plan and set your agency's privacy program, there are a number of preliminary steps you should take to make the process a smooth one:

- You should ensure that you are aware of your agency's **obligations under the Privacy Act and the Code**.
- You should **read this guide** and use **the tool on page six** to assess your agency's risk profile, which you can then use to **identify appropriate privacy maturity targets** for your agency.
- Finally, you should read the **Privacy Program Maturity Assessment Framework (Maturity Framework)** contained in Appendix 1 of this guide which forms part of the Interactive PMP. The Maturity Framework will help you to plan your agency's path to privacy maturity and determine achievable, measurable goals for your agency.

## What is a Privacy Management Plan (PMP)?

A PMP is a document that identifies specific, measurable privacy goals and targets and sets out how an agency will meet its compliance obligations under Australian Privacy Principle (**APP**) 1.2. Under the Code, an agency must:

- have a PMP (Code, s 9(1)); and
- measure and document its performance against its PMP at least annually (Code, s 9(3)).

## What is the Interactive PMP?

The Interactive PMP is an Excel based tool that has been designed by the OAIC to introduce efficiency into PMP development, measurement and documentation processes. It establishes a common framework for agencies to assess their maturity, identify compliance gaps and plan their privacy management activities for the coming year.

## Measuring maturity

The Interactive PMP includes a privacy program maturity assessment. The maturity assessment is intended to set common benchmarks across the public sector whilst using a scalable, risk-based approach. The maturity assessment in the Interactive PMP is based on the Maturity Framework contained in Appendix 1 of this guide.

## Interactive PMP: An overview

The Interactive PMP is broken down into the following steps:

- **Background**

In this step, the user sets the context for the PMP by providing information about their agency, the commencement and review dates for the PMP, and details about their agency's privacy risk profile.

- **Step 1: Measure maturity**

In this step, the user completes a risk-based maturity assessment of their agency based on the Maturity Framework (see Appendix 1). This step enables each agency to consider how well it has implemented its privacy program to date and to identify any gaps or opportunities. The Interactive PMP automatically highlights any maturity gaps which indicate a compliance issue under the Privacy Act or Code. In this step, the user also assesses the adequacy of their agency's privacy policy and notices, as required by the Code, s 17.

- **Step 2: Set your agency's actions**

- **Step 2A: Set compliance actions**

When the user moves to Step 2A, they will find that any compliance gaps they identified in Step 1 have been used to automatically populate remedial actions that their agency must take. The user records responsibilities, due dates and required resources for each action.

- **Step 2B: Set privacy policy and notices actions**

In this step, the user records the actions their agency will take to address any gaps in its privacy policy and privacy notices that were identified in Step 1.

- **Step 2C: Set actions for improving maturity**

In this step, the user records any actions their agency will take to meet its privacy maturity targets that were identified in Step 1.

Once the user has completed these steps, the PMP will be fully populated and ready to be actioned.

- **Step 3: Measure and document your agency's performance**

This step will be completed later in the year, when the agency reflects on how well it has

delivered against its PMP over the preceding year. In Step 3, users will measure and document their agency's performance and identify any gaps which must carry over to the next PMP. This step will help an agency to meet its obligations under the Code, s 9.

## How do I access the Interactive PMP?

You can download the Interactive PMP from the OAIC website, save it locally and complete it. It includes a section which is suitable for printing (called the **Printable PMP**) which summarises the information you enter into the Interactive PMP in a format which is suitable for distribution among colleagues who do not have a technical understanding of privacy. The Printable PMP should assist you with engaging stakeholders and reporting to others within your agency.

## Is it compulsory to use the Interactive PMP?

It is not compulsory for your agency to use the Interactive PMP to meet its PMP obligations. Your agency may choose another methodology to develop a PMP and to measure and document its performance against that PMP. However, the Interactive PMP is a comprehensive way of considering how well your agency operationalises privacy, and planning for uplift where it is needed. It also provides insight into what the OAIC considers to be a mature privacy program (see the Maturity Assessment at Appendix 1) and is part of a common framework for privacy management planning across the public sector.

## When to use the Interactive PMP

The Interactive PMP is intended to be a living document which can be referred to and updated throughout the year. However, it is likely that you will focus on your PMP at the following times:

### 1. **During the year, to guide your agency's privacy management activities**

The PMP becomes your agency's business plan for privacy for the year, helping your agency to address compliance gaps and facilitate continuous improvement. You should return to the Interactive PMP at regular intervals throughout the year to record your agency's progress against its actions.

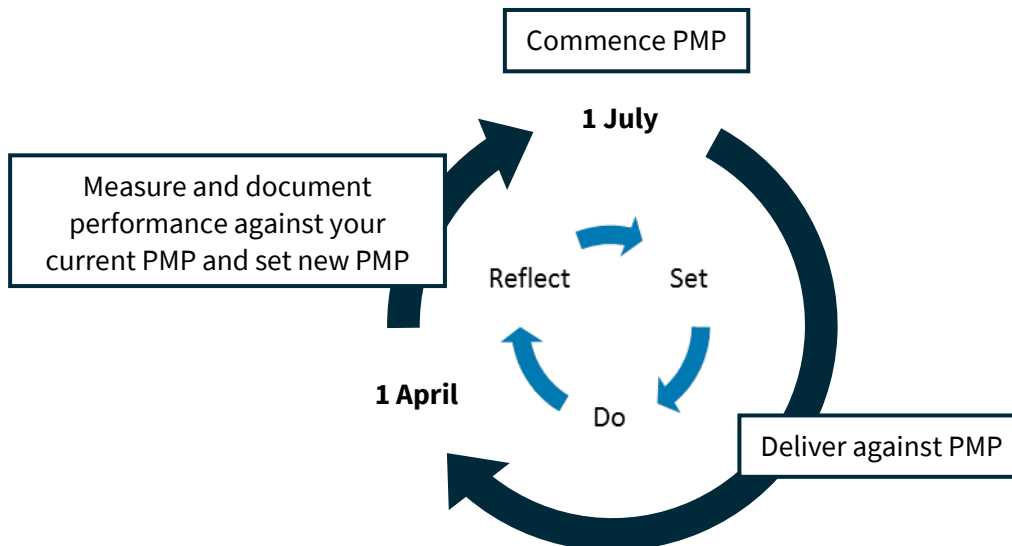
### 2. **In the last quarter of your agency's reporting year (whether that is a calendar year or a financial year)**

This is when you will reflect on your agency's current privacy program and consider how well your agency has met and delivered the targets set out in its current PMP (meeting the requirements of the Code, s 9(3)).

At this time, you will also create a fresh copy of the Interactive PMP and use it to reassess your agency's current state and develop your agency's PMP for the coming year. The outcomes of your agency's previous PMP will be relevant to the new PMP.

You should start the assessment process early enough to develop a strong PMP that can be endorsed by management and put into place by the start of the next year (for example, on 1 July). By completing this process in a timely way, you will be best placed to highlight priority activities for the coming year to senior management and seek the resources you will need to undertake them.

The diagram below illustrates a typical, annual PMP cycle. The dates in this diagram are indicative and your agency's reporting dates may be different.



## Who should complete the PMP?

The Privacy Champion is responsible for reviewing and/or approving the PMP annually (Code s 11 (4)). However, it is up to each agency to determine the most appropriate officer(s) to contribute to, co-ordinate, and manage the PMP obligations.

Many agencies will task their Privacy Officer(s) with the preparation of their PMP. Who is responsible for contributing to the PMP will depend on the size of the agency, the complexity of its processes and the level of detail you wish to cover. In a small agency, it may be possible for a single person to complete these actions but in a larger or more complex agency, a team of people may be required.

Ideally, any responsible staff member or team should have a combination of the following skills:

1. experience in undertaking audits, assessments or assurance activities; and
2. specialist knowledge of privacy and personal information management.

## Who should measure and document agency performance against the PMP?

Privacy Officers are responsible for measuring and documenting their agency's performance against the PMP at least annually (Code, s 10 (5)), which will need to be reviewed and/or approved by the Privacy Champion (Code, s 11 (4)). If some level of independence and impartiality is desired, you could consider engaging a third party to inform this review. This could include an independent assessor with the relevant skills or a peer agency (see more below about sharing your results and

working with other agencies). This is particularly relevant when assessing the maturity of the Privacy Officer role in the agency.

## Sharing your agency's PMP and working with other agencies

You may choose to share your agency's PMP (or parts of it, such as the maturity assessment) with other agencies with a view to sharing findings and resources that will enable your agency to meet its privacy obligations. You may also consider incorporating an agency peer review step into your agency's PMP cycle, to bring impartiality to your findings. Agencies that proactively share their PMP findings with the OAIC will be supported in their efforts to address gaps and implement improvements.

# Completing the Interactive PMP

## Background

### Information about your agency and key PMP dates

The Background step of the Interactive PMP requires you to identify your agency by name, and to specify the date that the PMP will commence. The Interactive PMP will then suggest a review period and end date for the PMP based on the values you have provided.

### Understanding your agency's privacy risk profile

The next part of the Background step requires you to identify your agency's privacy risk profile. This will help you to set targets and actions in your PMP which are appropriate for your agency. Remember, not all agencies need to aspire to be at Leader level.

Determining your agency's privacy risk profile requires an objective consideration of your agency's obligations under the Privacy Act, its activities and functions, the nature and volume of the personal information it holds, the nature of the agency (including its size and resources) and the sensitivity of the information. This is a similar process to determining what constitutes 'reasonable steps' for your agency to meet its obligations under APP 1.2 and APP 11. You may find that completing this exercise supports what you knew intuitively about your agency's approach to managing privacy or alternatively, that it highlights the need for uplift. You should ensure that you reach a well-supported conclusion on your agency's privacy risk profile.

The Interactive PMP provides space for you to record your agency's rationale for its privacy risk profile.

### Suggested privacy risk profile considerations

In determining your agency's privacy risk profile, it is recommended that you consider the matters described below, as well as any other factors relevant to your agency.

#### 1. Functions and activities

*An agency that administers payments or provides individualised services, will generally have a higher privacy risk profile than one which sets policies or provides infrastructure for the community at large, because handling personal information is a core function.*

- Does your agency provide public services to individuals or is it focused more on policy development?
- Does your agency provide services or support to individual members of the community?
- What sort of services does your agency deliver?
- Does your agency otherwise handle a lot of personal information, for example for research purposes?



## 2. Privacy influence and trust

*If your agency sets policy or delivers technology or services that will enable or materially impact the handling of personal information by others, it may have a higher privacy risk profile. Similarly, if your agency depends on the trust of the community to be successful, it may have a higher privacy risk profile.*

- Does your agency have a strong privacy influence (even if it does not hold personal information about members of the general public)?
- Does your agency rely on the trust of the community to meet its purposes?

## 3. Amount of personal information handled

*In considering this, you should have regard to the breadth (number of subjects) and depth (detail of personal information) in the data set. An agency with a large personal information holding will have a higher privacy risk profile than one with a small personal information holding.*

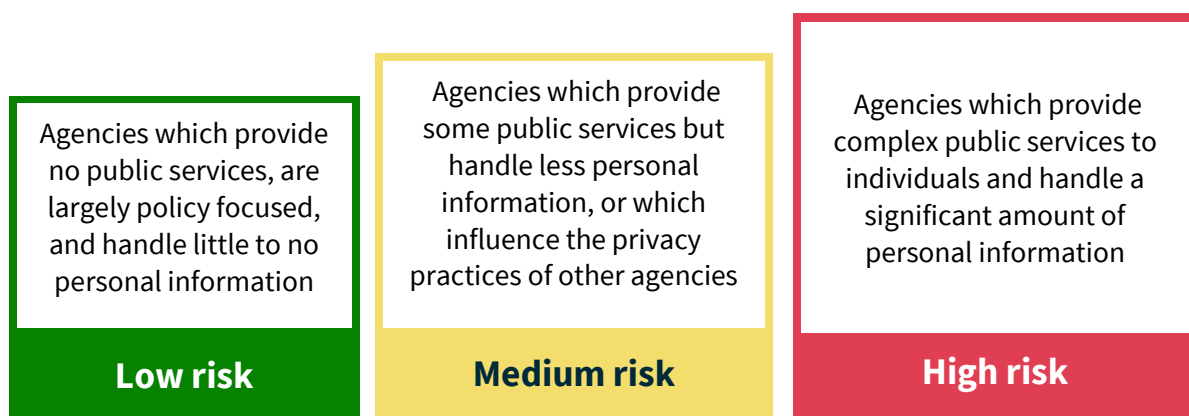
- Does your agency collect a significant amount of personal information, including personal information of employees?

## 4. Sensitivity of personal information handled

*In considering this, you should have regard to the sector of the community that your agency supports and its level of vulnerability. The greater the risk of harm to the individuals that your agency supports, the higher its risk profile.*

- Does your agency collect 'sensitive information' as defined in s 6 of the Privacy Act?
- Could the exposure of the personal information have harmful impacts on the affected individuals, whether or not it meets the definition of 'sensitive information'?

The following diagram gives some examples of the likely risk profiles of various agencies:

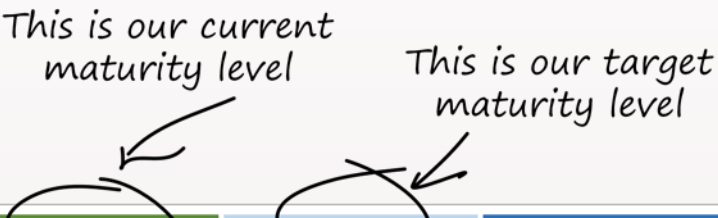


## Applying your privacy risk profile to set maturity targets

Once you have established your agency's privacy risk profile, you can identify the maturity level that your agency should aspire to. Based on your current maturity level assessment, you will identify gaps and set actions for maturity uplift in next year's PMP. You may find that certain attributes are more relevant to your agency and therefore have a higher target maturity level than others.

The maturity level that your agency targets will depend on a range of factors, including your agency's privacy risk profile. For example, an agency with a 'low risk' profile may decide that it only needs to meet its compliance requirements in relation to the 'Privacy Officer' attribute (and would therefore target the 'Developing' maturity level). On the other hand, an agency with a 'high risk' profile may determine that it needs to target the highest maturity level so that it can enhance and maintain public trust (and would therefore target the 'Leader' maturity level).

The following example shows how an agency that has self-identified as having a 'medium risk' profile might view the 'Privacy Officer' attribute in the maturity assessment and set its PMP accordingly.



Attribute	Initial	Developing	Defined	Leader
3. Privacy Officer*	No Privacy Officer in place <sup>2</sup> or the concept of Privacy Officer is notional only. For example, there is a 'privacy officer' email address but no systematised approach to who responds to emails directed to it.	<p>A Privacy Officer has been designated.</p> <p>The Privacy Officer is highly compliance-focused and has some practices, procedures and systems in place but these are generally siloed from broader organisational frameworks.</p> <p>Some staff are aware of the Privacy Officer.</p>	<p>The designated Privacy Officer has established practices, procedures and systems to support their obligations and these are documented and integrated into broader organisational frameworks.</p> <p>There is an agency wide awareness of the Privacy Officer.</p> <p>The Privacy Officer makes proactive privacy improvements which extend beyond compliance, and their performance is measured in this regard.</p>	<p>The designated Privacy Officer has established practices, procedures and systems that correlate with the agency's data governance, customer engagement and business transformation functions.</p> <p>The Privacy Officer is encouraged to innovate their practices, procedures and systems.</p> <p>The Privacy Officer willingly assists other agencies by sharing information and learnings about their role as privacy officer.</p>

## Step 1: Measure maturity

### Overview

There is a high degree of variability in how agencies (and other APP entities) implement privacy compliance obligations. The approach that each agency takes will depend on the level of awareness amongst staff and the leadership team, the agency's risk exposure and appetite and the resources that are available to personnel.

The Code introduces a range of privacy program requirements, including obligations to designate a Privacy Officer and Privacy Champion, to conduct privacy impact assessments and to develop and maintain a PMP. How each agency manages these obligations and the effectiveness of their approach will vary. In recognising this, the OAIC has developed the Maturity Framework as part of the Interactive PMP, to provide agencies with insight into what it considers the hallmarks of a mature privacy program.

The Maturity Framework is set out in full at Appendix 1 of this guide. The Interactive PMP gives the user a set of options to identify your agency's current and target maturity levels against the criteria set out in the Maturity Framework. These criteria are known as 'elements' and 'attributes'. The Interactive PMP will calculate your privacy maturity scores, first across each element by averaging out that element's attribute scores. Note that any non-compliant element – that is, an element with at least one compliance attribute (marked with an asterisk) that is rated at Initial – will have a score automatically restricted to Initial.

Then, the Interactive PMP will assess your overall privacy maturity across all elements and attributes to generate an overall privacy maturity score, and identify any compliance gaps. Your overall score will be rounded up or down to the nearest whole number, unless your score is below 1 – Initial. You can set targets to raise your agency's privacy maturity over the coming year as part of your PMP.

The Interactive PMP will flag where a low level of maturity is likely to indicate a compliance gap. By addressing these risks as a priority, you can minimise or eliminate your agency's exposure to privacy incidents and non-compliance with the Privacy Act. Compliance gaps identified in the maturity assessment are automatically transferred into your PMP actions for the coming year.

Completion of the maturity assessment will primarily involve gathering information about your agency's current privacy management practices. Methods to gather information might include:

1. interviews with management and staff;
2. gathering and reviewing documents;
3. site visits (where applicable); and
4. the use of workshops and/or surveys to understand roles, privacy risks and culture.

## Identifying your agency's current maturity levels

The Interactive PMP guides the user through the maturity assessment using the Maturity Framework (see Appendix 1). You will select your agency's current maturity level for each attribute on a four-point scale, from Initial (1), to Developing (2), to Developed (3), to Leader (4).

As shown below, an asterisk next to an attribute name, or a red cell, indicates that your agency may be non-compliant with its obligations under the Code or the Privacy Act. The Interactive PMP will also generate a maturity score for each element and across the maturity assessment. Any compliance gaps identified will be reflected in your element scores and will automatically populate in your PMP because these are the areas that must be addressed first.

Governance & Culture			
Attribute	Current Level	Target Level	Rationale/Commentary
Privacy Champion*	Initial		A red cell indicates a compliance gap. Elements with compliance gaps are automatically rated as 1 – Initial.
Privacy Values	Developing		
Privacy Officer*	Initial		
Management & Accountability	Initial		
Awareness	Developing		
Element score (average of attribute scores)			1 / 4 (Initial) – Compliance Gap

Governance & Culture			
Attribute	Current Level	Target Level	Rationale/Commentary
Privacy Champion*	Developing		
Privacy Values	Initial		
Privacy Officer*	Developing		
Management & Accountability	Initial		
Awareness	Developing		
Element score (average of attribute scores)			1.6 / 4 (Initial)

A score of 1.6 means that an agency's maturity level for this element is 'Initial' (1) but indicates there are some attributes which sit above 'Initial' (1).

## Setting your agency's target maturity levels

Once you have identified your agency's current maturity level for each attribute, you will decide its target maturity levels. Your agency should be selective about its targets and its resulting PMP to ensure that its goals are achievable. Which attributes are prioritised for uplift will depend on whether they are compliance gaps (these should be addressed first) as well as your agency's privacy risk profile and broader objectives.

The example below demonstrates an immature finding under 'Governance & Culture', with two attributes currently highlighted for non-compliance with the Code. Specifically, this agency has not designated a Privacy Champion (Code, s 11) or a Privacy Officer (Code, s 10). Its overall score for this element is 1.4 which means it has a maturity level of 'Initial' (as maturity is rounded down to the nearest whole number). If this agency has a high privacy risk profile, it is likely to need to uplift its maturity over the coming year, whereas if it has a low privacy risk profile, it may be sufficient simply to address the compliance gaps. In either case, the agency should prioritise its compliance actions in its PMP before deciding which other areas are to be targeted over the coming year.

Governance & Culture			
Attribute	Current Level	Target Level	Rationale/Commentary
Privacy Champion*	Initial	Developing	No executive leadership team member currently has any responsibility for privacy across the agency. This will help us to build a strong culture of privacy.
Privacy Values	Developing	Developing	We will review our privacy values this year to ensure they are up to date and make statements between agencies protecting privacy. We expect our current maturity level to remain the same.
Privacy Officer*	Initial	Developing	This is a compliance issue that we must prioritise. We have some staff who might consider privacy as part of their wider role, no one staff member has clear responsibility for this.
Management & Accountability	Initial	Developing	This is a weakness we need to focus on to ensure that our foundations are strong enough to grow our privacy function and to improve our privacy values in future years.
Awareness	Developing	Developing	We have basic awareness program but our staff tend to view privacy as a compliance issue. We will focus on improving other capabilities this year.
Element score (average of attribute scores)			1.4 / 4 (Initial)

This agency is planning to improve its maturity in these areas.

**Assessing the adequacy of your agency's privacy policy and notices**

Section 17 of the Code requires an agency to regularly assess the adequacy of its privacy practices, procedures and systems (including its privacy policy and collection notices) to ensure their adequacy for the purpose of compliance with the APPs and currency. Completing this step in the Interactive PMP facilitates compliance with this requirement.

## Step 2: Set your agency's actions

The next step in the Interactive PMP is to set your agency's actions for the coming year. In this step you should consider the following:

- Any compliance gaps: actions which close compliance gaps should be given immediate priority. Compliance gaps are flagged in Step 1 and appear in Step 2 with a space for you to input your remediation actions.
- Any other obligations that you are required to address under the Code or the Privacy Act should be addressed. For example, under the Code, s 17, you must regularly review and update your privacy practices, procedures and systems, to ensure their currency and adequacy for the purposes of compliance with the APPs. The scope of the review must include any privacy policy prepared for the purposes of APP 1 and privacy notice prepared for the purposes of APP 5. Any gaps you identify as part of these reviews will require action and should be captured in the PMP.
- Your agency's privacy risk profile and maturity targets: Actions which help your agency to address its maturity targets should be addressed.

The Interactive PMP will direct the user to address each of the above areas. The tool is flexible in that users can add more lines to the PMP and cover additional areas as required. Blank lines will automatically drop out when you print the PMP from the tool.

### SMART goals

You should ensure that actions in your agency's PMP are 'SMART', which is an acronym for Specific, Measurable, Attainable, Realistic and Timely. Smart goals are clear, which makes them easier to achieve. By setting smart goals you can ensure that all stakeholders understand what is required, which goals take priority for the agency and their responsibilities in achieving them. When it comes time to measure and document your agency's performance under your PMP (Code, s 9), smart goals are also easier to assess.

### Communicate within the agency

Once you have completed your PMP, you should ensure that you follow your agency's usual reporting and governance procedures. By ensuring that senior staff (including the Privacy Champion) are engaged, you will be more likely to succeed in implementing the actions in the PMP over the coming year. This also ensures that your privacy program is integrated into your agency's reporting, assurance and accountability frameworks (itself an indicator of maturity).

Make sure you also communicate the PMP back to any stakeholders who were involved in the maturity assessment or other aspects of setting the PMP. These people have an interest in the plan and may be required to act to lift privacy practice in their business area. They will want to know where they sit and what they need to do next. This information might also be relevant to their own performance and KPIs, and sharing it is a practical step you can take to help build a privacy aware culture in your agency.

## Step 3: Measure and document your agency's performance

Each year, your agency is required to measure and document its performance under its PMP (Code, s 9). It is good practice to maintain the PMP as a living document and to supplement the annual review by updating your PMP throughout the year. For example, as actions are completed, you can close them on the PMP. Remember not to delete these items as the PMP document should stand as a record of the actions your agency has taken over the year.

The actions that you have set through steps 2A, 2B and 2C of the Interactive PMP are presented in summary form in Step 3. Alongside each action, there is a drop-down option to record whether it has been achieved, and a space to record any future actions or commentary associated with the action.

**PMP end date** Following commencement, this PMP will operate until Sunday, 30 June 2019.

**Recommended review period** Monday, 1 April 2019 to Sunday, 30 June 2019

**PMP review date**

Action	Achieved	Future actions / commentary
Document categories of personal information collected, used and disclosed, including any offshore recipients.	Yes	The Records Manager completed this action on 14 July 2018. The resulting documentation is available to the Privacy Officer and risk staff for consideration when Privacy Impact Assessments or otherwise as risk. The resulting information was also used in DWP's risk register, and was checked against policy and privacy notices for currency (updates required).
Define processes to monitor and improve the quality of personal information and ensure these are regularly undertaken.	Partially	The Records Manager has distributed a draft process manual which is currently being reviewed by stakeholders. It is expected to be finalised by the end of August 2018.
Develop a privacy training programme and ensure this is delivered to staff on induction and annually.	Partially	

Action status can be recorded as 'Yes', 'No' or 'Partially'.

Agencies can record how they achieved an action and future steps.

When the time comes to start preparing your agency's next PMP, the results which you have recorded in step 3 of your agency's previous PMP will help you to assess your agency's privacy maturity levels and to determine realistic target maturity levels. Any actions from your agency's previous PMP that weren't achieved should be carried forward to the new PMP, if they are still relevant to your agency's target maturity levels.



## Case study: Department of Workforce Planning



In this section, we will follow the experience of fictional agency, the Department of Workforce Planning (**DWP**) in using the Interactive PMP to assess its maturity, set its PMP and measure and document its performance against its PMP. Although DWP is fictional, the privacy risks that DWP faces and its considerations in developing a PMP reflect the experiences of many real agencies.

### About DWP

DWP is responsible for overseeing and coordinating the federal government's approach to workforce planning and investment. For example, DWP conducts research into commercial, economic and geographic employment trends and challenges and advises the government on future workforce needs.

The primary function of DWP is to support a prosperous Australian economy via sound workforce planning. DWP holds a large amount of aggregated, de-identified data about Australia's current workforce and has access to statistical analysis undertaken by other entities.

### DWP's privacy risk profile

DWP primarily works with de-identified data and collects only a small amount of personal information itself. Its main personal information holding consists of records of focus groups and surveys it conducts several times a year, where the size of the research participant group tends to be small (less than 500 participants). It does not collect 'sensitive information' as defined under the Privacy Act, s 6. Apart from this, a small team of DWP's research staff can access personal information held in the databases of two related agencies. DWP only uses statistical findings to advise on workforce planning, never personal information. On this basis, DWP has rated its privacy risk profile as low.

### Focus areas for DWP

Due to DWP's role in the formation of nationwide economic policy and its high public profile, a privacy breach could seriously damage DWP's reputation and may deter individuals from participating in focus groups and surveys. A breach could also damage its relationship with the agencies whose data it uses. For these reasons, DWP wants to ensure that it has established a solid governance framework for privacy and data protection, and ensure that it has implemented privacy practices, procedures and systems that are sufficiently robust to withstand internal or external threats that may lead to data breaches. It views good privacy governance as an essential part of maintaining community trust and its partnerships with other agencies.

## Completing the Interactive PMP for DWP

### Background

In this step, DWP has provided some background information about itself and the planned commencement date for this PMP. DWP has determined that its privacy risk profile is low, and in this step it has recorded some of the matters that were considered in reaching that conclusion.

The excerpt below shows some of DWP's responses in the Background step.

#### About this PMP

<b>Agency name</b>	Department of Workforce Planning
<b>PMP commencement date</b>	1/07/2018 <i>It is recommended that Agencies commence a new PMP on 1 July every year.</i>
<b>PMP end date</b>	Following commencement, this PMP will operate until Sunday, 30 June 2019.

#### Your agency's privacy risk profile

It is assumed that you have already identified your agency's privacy risk profile using the process described in Interactive PMP Explained. If you haven't completed this exercise, it is recommended that you do so before proceeding with the Interactive PMP. Suggestions for relevant considerations are provided in Interactive PMP Explained.

You can record your agency's rationale for its privacy risk profile in the space below.

<b>Privacy risk profile rationale</b>	<p>DWP is purely focused on policy development. It does not provide services to individual members of the public.</p> <p>DWP is responsible for overseeing and coordinating the federal government's approach to workforce planning and investment. For example, DWP conducts research into commercial, economic and geographic employment trends and challenges and advises the government on future workforce needs. Even though DWP only handles small volumes of personal information, it relies on the trust and goodwill of the community for the free flow of useful data.</p>
---------------------------------------	---

### Step 1: Measure maturity

In this step, DWP has assessed its current privacy maturity using the Maturity Framework and identified gaps and opportunities for uplift.

The excerpt below shows some of DWP's responses in its maturity assessment.

Governance & Culture			
Attribute	Current Level	Target Level	Rationale/Commentary
Privacy Champion*	Developing	Developing	As DWP has a low privacy risk profile, it is satisfactory to have a maturity level of Developing. A Privacy Champion has been designated and undertakes some activities to promote a culture of privacy that values and protects personal information. The Privacy Champion provides leadership on broader strategic privacy issues.
Privacy Values	Initial	Developing	At the moment there is no connection between the agency's values and privacy. We will review this over the coming year to ensure that we can articulate and make staff aware of the link between agency values and protecting privacy.
Privacy Officer*	Developing	Defined	The Privacy Officer is primarily focused on compliance and has some practices, procedures and systems in place. There are opportunities to better integrate privacy into broader organisational frameworks and raise awareness of the Privacy Officer.

In this step, DWP has also reviewed its privacy policy and collection notices to ensure that they are adequate for the purposes of the APPs, and that they are up to date.

The excerpt below shows DWP's findings in relation to its privacy policy and privacy notices.

	Compliance Gaps (if any)	Currency Gaps (if any)
Privacy Policy (APP 1)	Does not set out how an individual may access personal information held by DWP and seek its correction.	Does not cover DWP's practices in relation to focus groups and surveys, activities which have only commenced in the last year. DWP collects personal information when it conducts these activities.
Privacy Notices (APP 5)	DWP does not routinely issue privacy notices and does not have a policy of issuing privacy notices at or before the time or as soon as practical after collection of personal information about an individual.	Nil

## Step 2: Set actions

In steps 2A, 2B and 2C, DWP will set its PMP actions, including those required to close compliance gaps, address gaps identified in its privacy policy and privacy notices and lift the maturity of DWP, based on its maturity targets for the coming year. Once the user has completed these steps, the PMP will be ready for DWP to use in the coming reporting year.

The excerpt below shows some of DWP's responses in step 2A, where it recorded its remediation actions for dealing with the compliance gaps identified in the maturity assessment. The Interactive PMP displays suggested actions for dealing with each compliance gap, and DWP has adopted the suggested actions in full.

Attribute / Suggested action	Remediation action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents
<b>Inventory of Personal Information</b>  <b>Suggested action:</b> Document categories of personal information collected, used and disclosed, including any offshore recipients.	Document categories of personal information collected, used and disclosed, including any offshore recipients.	Records Manager with input on privacy requirements from Privacy Officer	1/08/2018	N/A
<b>Data Quality Processes</b>  <b>Suggested action:</b> Define processes to monitor and improve the quality of personal information and ensure these are regularly undertaken.	Define processes to monitor and improve the quality of personal information and ensure these are regularly undertaken.	Records Manager with input on privacy requirements from Privacy Officer	1/09/2018	N/A
<b>Privacy Training</b>  <b>Suggested action:</b> Amend the induction programme to include a privacy training component and ensure this is delivered to staff on induction and annually.	Amend the induction programme to include a privacy training component and ensure this is delivered to staff on induction and annually.	Head of HR to procure or develop eLearning privacy component for induction programme. Privacy Officer to provide interim face to face training.	1/10/2018	Funding is required for eLearning materials

The excerpt below shows some of DWP's responses in step 2B, where it recorded how it would handle the compliance and currency gaps in its privacy policy and privacy collection notices.

Gap type	Remediation action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
Privacy Policy (APP 1)	Privacy Policy needs to be amended to explain how individuals can seek access and correction.	Privacy Officer	1/07/2018	Legal is a key stakeholder and will need to give input on the policy and template.
Privacy Policy (APP 1)	Privacy Policy needs to be amended to cover DWP's conduct of focus groups and surveys and resulting collection and handling practices.	Privacy Officer	1/07/2018	Legal is a key stakeholder and will need to give input on the policy and template.
Privacy Notices (APP 5)	DWP needs a policy which explains when a privacy notice should be issued. DWP will also develop a template privacy notice and a process whereby the draft privacy notice is reviewed by Legal before it is published.	Privacy Officer	1/07/2018	Legal is a key stakeholder and will need to give input on the policy and template.

In step 2C, DWP was presented with a table summarising the maturity improvements goals that it set for itself in the maturity assessment, along with a suggested outcome for each goal and a blank space to record an action for achieving that outcome. The excerpt below shows some one of these improvement goals, and DWP's planned action for meeting it. Improvement goals which would simply meet a compliance requirement are not shown in this step, because they have already been addressed in step 2A.

Element / Attribute	Current Level	Target Level	Suggested Outcomes	Action
Governance & Culture / Privacy Values	Initial	Developing	There is a connection between the agency's values and respecting and protecting personal information. This connection is understood by staff.	Privacy Officer to develop a privacy fact sheet which links the agency's values to its privacy obligations and targets. Privacy Champion to distribute and promote the fact sheet.

Step 2C also provides a space for recording more details for each improvement action. The improvement actions entered above are automatically carried into this table. In the excerpt below, DWP has provided additional details for the action that it described immediately above.

Element / Attribute	Action	Responsible person, position or team	Due	Required resources, dependencies and/or related documents (specify or link)
Governance & Culture / Privacy Values	Privacy Officer to develop a privacy fact sheet which links the agency's values to its privacy obligations and targets. Privacy Champion to distribute and promote the fact sheet.	Privacy Officer, Privacy Champion	1/12/2018	An additional resource is required to assist with drafting. This could be a secondee from another part of the agency or an external consultant if budget can be found.

At the bottom of step 2C, there is space to provide additional improvement actions that are outside of the Maturity Framework.

### Step 3: Measure and document your agency's performance

In this step, DWP will reflect on how well it has delivered against its PMP over the preceding year and identify any actions which must carry over to the next PMP. DWP has set a review date for the PMP, which is the date when it will begin to assess its overall progress for the reporting year, as a first step in preparing a new PMP for the following year. However, the Privacy Officer and others should keep the records of how DWP is progressing against its actions up to date throughout the year.

The excerpt below shows some of the records of DWP's actions several months into the reporting year.

<b>PMP review date</b>		1/04/2019
Action	Achieved	Future actions / commentary
Document categories of personal information collected, used and disclosed, including any offshore recipients.	Yes	The Records Manager completed this action on 14 July 2018. The resulting documentation is available to the Privacy Officer and risk staff for consideration when carrying out Privacy Impact Assessments or otherwise assessing privacy risk. The resulting information was also used to update DWP's risk register, and was checked against DWP's privacy policy and privacy notices for currency (updates were not required).
Define processes to monitor and improve the quality of personal information and ensure these are regularly undertaken.	Partially	The Records Manager has distributed a draft process manual which is currently being reviewed by stakeholders. It is expected to be finalised by the end of August 2018.

## Additional actions

- DWP's Privacy Officer completes the initial maturity assessment and drafts the PMP between April and May of the current year, with a view to it commencing on 1 July. This accords with DWP's planning cycle and gives the Privacy Officer enough time to brief the Privacy Champion, obtain formal endorsement of the PMP and influence budget setting for the year ahead.
- Around this time, DWP's Privacy Officer also circulates the PMP (including the maturity findings) to the stakeholders who were involved in gathering information and working through the assessment and goal setting in the PMP. Responsibility for some of the actions in the PMP will lie with those stakeholders and hence, they have an interest in the final document.
- The Privacy Officer also publishes an awareness article about the process on DWP's online notice board and during Privacy Awareness Week hosts a briefing for staff to hear about privacy management at DWP. This helps to drive a privacy aware culture and the Privacy Officer notes this as an example of action taken to uplift awareness on the PMP.
- Over the year, DWP's Privacy Officer closes actions on the PMP that have been completed.
- In April of the following year, DWP's Privacy Officer prepares to measure and document the agency's performance against its PMP over the year to date. The Privacy Officer has already kept the document up to date, so the effort required to complete this task is minimal. The exercise indicates that there are a couple of actions which were not completed according to the PMP, and these are carried into the following year's PMP.
- As part of this process, DWP's Privacy Officer reassesses DWP's maturity (Step 1) and finds that it has lifted its overall maturity score from Initial to Developing.
- DWP works closely with another agency known as The Digital Workforce Agency (DWA), which is focused on research and development in workforce technology. DWA has also recently completed its annual review of its performance against its PMP. As the two agencies often work closely together, the respective Privacy Officers agree to share their draft findings to bring an element of objectivity to the assessment process. The maturity findings and new targets are carried into the following year's PMP.

# Appendix 1: Privacy Program Maturity Assessment Framework

## Overview

The Privacy Program Maturity Assessment Framework (**Maturity Framework**) supports the requirements of the *Privacy (Australian Government Agencies — Governance) APP Code 2017 (Code)* by giving agencies a framework to assess their privacy maturity across a set of objective criteria.

The Maturity Framework is a scalable, risk-based tool in that it does not require every agency to strive for best practice. Rather, an agency may choose to aim to reach a maturity level that is proportionate to its privacy risk profile. By actively understanding their own risk exposure and maturity level relative to others, and by setting goals and targets on an annual basis, agencies can adopt a proactive approach to maintaining internal practices, procedures and systems as required by APP 1.2 (and other APPs).

## Maturity assessment — key concepts

### Five elements of maturity

The Maturity Framework consists of five elements, each of which are critical tenets of APP 1.2 and Code compliance, and constitute good privacy practice. The five elements are:

#### 1. Governance & Culture

This element measures how well your agency has established robust governance structures for privacy and embedded privacy into its culture.

#### 2. Privacy Strategy

This element measures how well your agency has integrated privacy into other key information management disciplines.

#### 3. Privacy Processes

This element measures how fit-for-purpose, comprehensive and effective your agency's key privacy processes are.

#### 4. Risk & Assurance

This element measures how well-developed your agency's privacy risk and assurance processes are.

#### 5. Data Breach Response

This element measures how ready your agency is to handle a data breach and to learn from it.



## Attributes

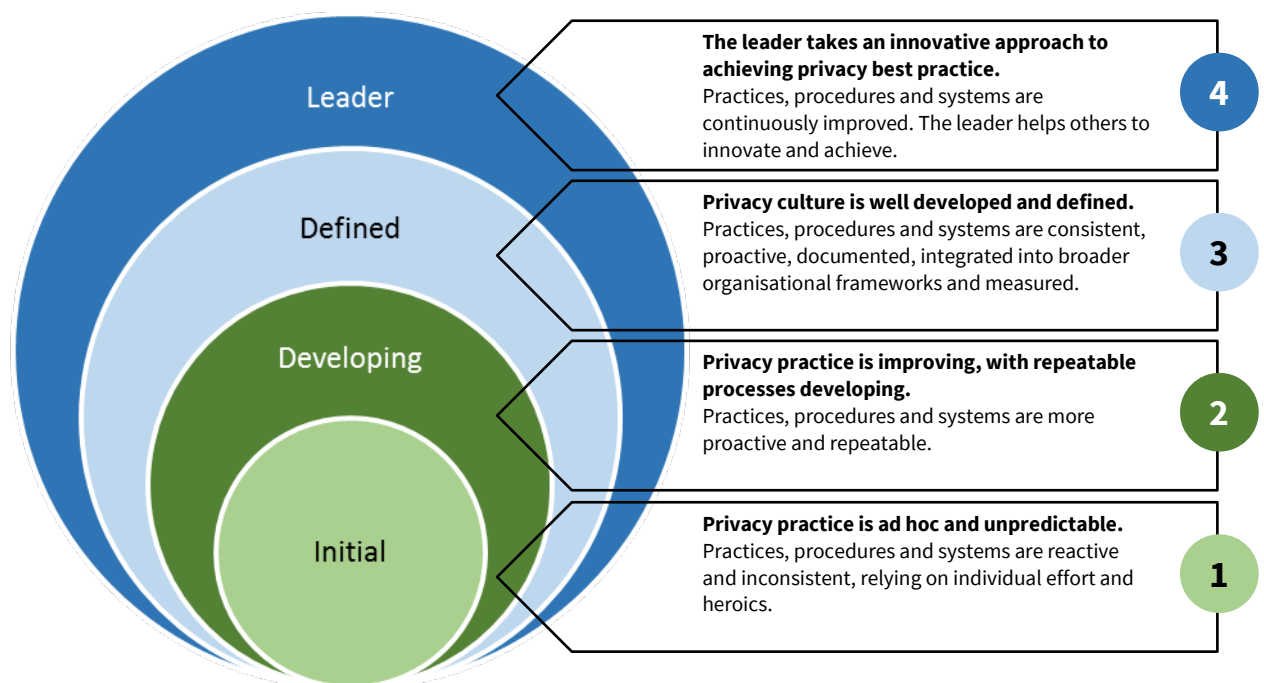
Within each element sits a set of attributes. Attributes are the criteria against which you can measure privacy maturity. For example, the attributes under the 'Governance & Culture' element are:

1. Privacy champion
2. Privacy values
3. Privacy officer
4. Management and accountability
5. Awareness

There is a total of 21 attributes under 5 elements.

## Four cumulative maturity levels

The Maturity Framework requires the user to assess their agency's maturity across four maturity levels. The maturity levels are shown in the following diagram:



## Detailed maturity descriptors

The attributes for each maturity level within the Maturity Framework are described in detail below. An asterisk (\*) next to an attribute name means that it is a 'compliance attribute' and that an agency must have a minimum maturity level of 'Developing' to comply with the Privacy Act or the Code.

### 1. Governance and culture

This element measures how well your agency has embedded privacy into its culture and established robust governance structures. An agency can effectively achieve a privacy aware culture by ensuring that staff understand how privacy correlates with the agency's values and strategic direction and by reflecting these values at a practical level in the agency's practices, procedures, and systems. The more effective the privacy culture, the more mature that agency will be. An agency that views privacy as a box-ticking exercise or treats it in isolation from broader organisational frameworks does not have a mature privacy culture, and this can expose the agency to greater legal or reputational risks.

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>1. Privacy Champion*</b>	<p>No Privacy Champion in place.<sup>1</sup></p> <p>There is no one in the agency at a senior level with responsibility for promoting a culture of privacy that values and protects personal information.</p>	<p>A Privacy Champion has been designated.</p> <p>The Privacy Champion undertakes some activities to promote a culture of privacy that values and protects personal information.</p> <p>Privacy management is undertaken strategically with the Privacy Champion providing leadership on broader strategic privacy issues.</p>	<p>The designated Privacy Champion consistently promotes a culture of privacy that values and protects personal information and supports the integration of privacy practices, procedures and systems into broader organisational frameworks.</p> <p>The performance of the Privacy Champion is measured as a KPI.</p>	<p>The designated Privacy Champion actively seeks opportunities to improve the privacy culture of the agency.</p> <p>The performance of the agency in relation to privacy is a KPI for the Privacy Champion.</p> <p>The Privacy Champion has a mandate to engage and speak publicly on relevant issues.</p>

<sup>1</sup> Does not comply with the Code.

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>2. Privacy Values</b>	There is no connection between the agency's values and respecting the information and privacy of individuals with whom the agency engages.	There is a connection between the agency's values and respecting and protecting personal information. This connection is understood by staff.	<p>The agency's documented values clearly promote a culture of respecting and protecting personal information to build trust.</p> <p>The agency's PIA and privacy evaluation processes incorporate an assessment of how the initiative aligns to the agency's values.</p>	The agency publicises its values which promote a culture of valuing and protecting personal information.
<b>3. Privacy Officer*</b>	No Privacy Officer in place <sup>2</sup> or the concept of Privacy Officer is notional only. For example, there is a 'privacy officer' email address but no systematised approach to who responds to emails directed to it.	<p>A Privacy Officer has been designated.</p> <p>The Privacy Officer is highly compliance-focused and has some practices, procedures and systems in place but these are generally siloed from broader organisational frameworks.</p> <p>Some staff are aware of the Privacy Officer.</p>	<p>The designated Privacy Officer has established practices, procedures and systems to support their obligations and these are documented and integrated into broader organisational frameworks.</p> <p>There is an agency wide awareness of the Privacy Officer.</p> <p>The Privacy Officer makes proactive privacy improvements which extend beyond compliance, and their performance is measured in this regard.</p>	<p>The designated Privacy Officer has established practices, procedures and systems that correlate with the agency's data governance, customer engagement and business transformation functions.</p> <p>The Privacy Officer is encouraged to innovate their practices, procedures and systems.</p> <p>The Privacy Officer willingly assists other agencies by sharing information and learnings about their role as privacy officer.</p>

<sup>2</sup> Does not comply with the Code.

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>4. Management &amp; Accountability</b>	<p>It is unclear who has overall senior management accountability for privacy within the agency.</p> <p>There is inadequate resourcing for managing privacy compliance activities (for example, handling internal and external privacy enquiries, complaints, and access and correction requests).</p> <p>Privacy management is reactive.</p>	<p>The agency has assigned responsibility for privacy compliance including senior oversight and operations.</p> <p>There is adequate resourcing for managing privacy compliance activities (for example, handling enquiries, complaints, and access and correction requests).</p> <p>Some staff are aware of privacy accountabilities and how to seek assistance.</p>	<p>Roles and accountabilities for privacy compliance and oversight are documented and well understood across the agency, and messaging regarding roles and accountabilities is tied to the agency's broader strategic objectives.</p> <p>The agency regularly measures its performance in relation to privacy management (for example, timeliness and quality) and seeks to implement learnings for continuous improvement.</p>	<p>Measurement of the agency's performance and continuous improvement initiatives are undertaken and reported to senior management regularly.</p> <p>The agency is transparent with the public about who holds accountability for privacy within the agency and its management and accountability practices.</p>
<b>5. Awareness</b>	<p>Staff have little to no awareness of privacy. Some rights and obligations are viewed negatively. Privacy is generally viewed as a barrier.</p>	<p>Staff view privacy neutrally as a compliance issue. There is a developing appreciation of the importance of privacy.</p>	<p>Staff view privacy as a positive and valuable part of business as usual.</p> <p>There is strong knowledge of agency policies and expectations.</p> <p>Staff are encouraged to take opportunities to provide feedback on the agency's privacy processes (via established channels such as suggestion boxes and staff meetings).</p>	<p>Staff view privacy as an enabler.</p> <p>Staff know how to apply agency privacy policies and expectations to emerging issues.</p> <p>The agency is willing to share its awareness resources with others or to work together to develop sectoral resources which meet the needs of the sector, as well as the specific needs of each agency.</p>

## 2. Privacy Strategy

This element measures your agency's strategic approach to privacy, which includes how well your agency is integrating privacy into other key information disciplines. The Maturity Framework recognises that personal information is a valuable business asset, and optimising its use and usefulness can be critical to the successful delivery of agency functions. Under this element, you will assess how well personal information assets are understood, respected, managed and protected across the agency, not just within the privacy function.

*Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.*

Attribute	Initial	Developing	Defined	Leader
<b>6. Privacy Management Plan*</b>	No Privacy Management Plan in place. <sup>3</sup>	<p>The agency has a Privacy Management Plan in place and some staff are aware of it.</p> <p>The Privacy Management Plan includes measures for addressing any known privacy compliance gaps.</p>	<p>Senior management and key staff are aware of the agency's Privacy Management Plan and the agency's primary objectives under it.</p> <p>The Privacy Management Plan is considered when setting resourcing budgets for the year ahead.</p> <p>The Privacy Management Plan addresses the handling of personal information throughout the information lifecycle with specific consideration given to areas that the agency assesses as having greater risk. It also includes actions to improve privacy maturity outcomes.</p>	<p>The agency publishes its Privacy Management Plan and its progress against it.</p> <p>The agency's focus on innovation is apparent in its Privacy Management Plan.</p>

<sup>3</sup> Does not comply with the Code.

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>7. Inventory of Personal Information*</b>	The agency does not know what personal information it holds. <sup>4</sup>	The agency has documented the general categories of personal information that are collected, used and disclosed by the agency. It describes the purposes for which the information is collected and how it is stored (such as whether it is stored overseas, with a cloud service provider or other third party).	<p>The agency has documented its personal information holdings, and understands all data flows in and out of the agency (including where third parties hold that information).</p> <p>Ownership, accountability and access for specific IT systems and databases that hold personal information are clear and documented. The record also details how long the information will be retained and when it will be de-identified and destroyed.</p> <p>The agency has implemented processes that routinely monitor changes to its personal information holdings.</p>	<p>The agency considers the documentation of personal information holdings in the context of its broader organisational goals and priorities. It harnesses the record to identify opportunities to maximise uses of data and to manage relevant risks.</p> <p>An innovative and sophisticated approach is taken to the development of the IT system which houses the record of personal information holdings.</p> <p>The agency proactively publishes their record where appropriate, and shares its insights and advice with other agencies.</p>

<sup>4</sup> Does not comply with the Code.

*Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.*

Attribute	Initial	Developing	Defined	Leader
<b>8. Data Quality Processes*</b>	The agency has no processes in place to monitor or improve the quality of personal information. As a result, it holds a lot of personal information which is incomplete, inaccurate, out of date or irrelevant to the agency's functions.	The agency is starting to define processes to monitor and improve the quality of personal information and these are regularly undertaken.	<p>The need to maintain the quality of personal information is understood not only as a privacy concern but as a strategic objective for the agency in the context of its broader functions, which all staff play a part in delivering.</p> <p>New procedures and systems offered by the agency routinely empower individuals to keep the personal information that the agency holds about them complete, accurate and up to date.</p>	<p>The agency regularly investigates and takes opportunities to innovate its processes for ensuring the quality of personal information.</p> <p>The agency willingly assists other agencies to improve their data quality processes by sharing its learnings.</p>

<p><b>9. Information Security Processes</b></p>	<p>There is limited awareness of the agency's information security obligations amongst staff.</p> <p>The information security function is largely siloed from privacy and other functions.</p> <p>The agency has no documented data retention policy in place.</p>	<p>The agency has a developing information security-aware culture.</p> <p>Information security policies and procedures, including retention policies, for all staff are emerging.</p> <p>The agency's information security staff routinely collaborate with the Privacy Officer and other individuals with privacy accountabilities and there is a good level of understanding between them of how privacy and security fit together.</p>	<p>The agency has an established information-security aware culture.</p> <p>Staff understand the commonalities and differences between privacy and security and are aware of all relevant privacy and security policies and processes.</p> <p>Policies and processes relating to mutual risks and issues (such as data breaches, access controls, appropriate use of technology, workplace surveillance, retention etc.) integrate privacy and security requirements with clear hand off processes to reduce delay and duplication of effort by stakeholders.</p> <p>Where archiving obligations prevent de-identification or destruction of personal information, it is agency policy to adopt other measures to limit privacy risks (such as archiving and limiting access to those personal information holdings).</p>	<p>The agency willingly assists other agencies by sharing experiences and insights which encourage better collaboration between information security, privacy and other functions.</p>
---	--	---	---	--



### 3. Privacy processes

This element measures how fit-for-purpose, comprehensive and effective your agency's key privacy processes are. The way these processes are viewed by your agency says a lot about its privacy maturity. For example, an agency that views individual access and correction rights negatively is likely to have issues with privacy culture more generally. The more embedded a process is across the agency (that is, the stronger the understanding of privacy rights and processes by all staff), the more mature that agency will be.

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>10. External Privacy Policy and Notices*</b>	<p>No privacy policy or other messaging is provided to the public.<sup>5</sup></p> <p>Privacy messaging is viewed negatively, as a burden and an encroachment on agency secrecy.</p> <p>Privacy notices are not always provided where personal information is collected.<sup>6</sup></p>	<p>Privacy messaging is viewed neutrally as a compliance requirement but is not prioritised.</p> <p>A privacy policy is provided to the public. The policy is compliance-focused, and provides the information required by APP 1.4.</p> <p>Privacy notices are provided where personal information is collected. Notices are compliance-focused, providing the information required by APP 5.2, and can be legalistic.</p> <p>Privacy messaging is inconsistent and can be difficult to locate.</p>	<p>Privacy messaging is viewed positively as an important part of the agency's privacy practice.</p> <p>A clear, comprehensive and plain English privacy policy is provided to the public and goes beyond compliance, focusing on customer experience, openness and transparency.</p> <p>There is a clear link between privacy notices, and the privacy policy and privacy messaging is consistent and easy to locate.</p>	<p>Privacy messaging is viewed as an opportunity to build trust and engage the public.</p> <p>Innovative approaches are taken to deliver privacy messaging to the public, such as the use of infographics, animation or video or other forms of technology to increase user experience.</p>

<sup>5</sup> Does not comply with the APPs.

<sup>6</sup> Does not comply with the APPs.

*Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.*

Attribute	Initial	Developing	Defined	Leader
<b>11. Internal Policies and Procedures</b>	<p>No identifiable internal privacy policies or procedures in place.</p> <p>There are no documents that explain to staff the agency's privacy obligations or how privacy might be relevant to the agency's functions.</p> <p>Privacy is not a consideration in broader risk management analyses or documents.</p>	<p>Some internal privacy policies and procedures in place but they are not comprehensive and are highly compliance-focused and poorly operationalised.</p> <p>Some staff are aware of these policies and procedures, but they may not be consistently followed.</p> <p>Internal privacy policies and procedures are regularly reviewed to ensure compliance with current law or relevance to agency practices.</p>	<p>Clear, relevant and comprehensive internal privacy policies and procedures are in place.</p> <p>Internal privacy policies and procedures go beyond compliance and are well-operationalised.</p> <p>Staff are aware of these policies and procedures and they are followed consistently, resulting in a common approach to privacy across the agency.</p> <p>Internal privacy policies and procedures are proactively reviewed to ensure compliance with current law, community expectations and relevance to current agency practices and in response to privacy risks and opportunities.</p>	<p>Staff and management proactively contribute to improving internal privacy policies and procedures.</p> <p>Internal privacy policies and procedures are an integral part of the way that the agency functions.</p> <p>Innovative approaches are taken to design, distribute and embed privacy policies and procedures within the agency.</p> <p>Internal privacy policies and procedures are proactively reviewed to ensure that they encourage privacy best-practice and effectively change culture and behaviour.</p>

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>12. Privacy Training*</b>	<p>Limited or no privacy training provided to staff.<sup>7</sup></p> <p>No process in place to monitor privacy knowledge.</p>	<p>Training is provided to all staff on induction and annually.</p> <p>Training is compliance-focused and tends to target specific issues, such as information security and secrecy obligations without sufficient context or an explanation of broader privacy issues.</p> <p>Staff completion rates and understanding of privacy is not monitored unless there is a breach or complaint.</p>	<p>Training is operationalised to ensure relevance to all staff depending on their role and business unit.</p> <p>A clear and integrated training program is in place with regular opportunities for refresher or more specialised training (for example, on drafting a PIA as part of a change-management process).</p> <p>Training goes beyond compliance, is comprehensive, links to the agency's internal and external policies and messaging and is periodically updated</p> <p>Staff completion rates and understanding of privacy are monitored.</p>	<p>Training program links good privacy practice with other agency goals and priorities, such as customer experience and trust.</p> <p>Innovative approaches taken to training delivery, including a combination of training methods (such as online modules, workshops, simulations or practical sessions).</p> <p>The agency willingly assists other agencies to develop effective training programs including taking opportunities to run inter-agency training.</p>

<sup>7</sup> Does not comply with the Code.

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>13. Privacy Impact Assessments</b> *	No PIA process exists. <sup>8</sup>	<p>PIA process exists but it is only used for high privacy risk projects.</p> <p>Privacy issues which do not meet the high privacy risk threshold are rarely considered.</p> <p>Where PIAs are completed, they are run by privacy or risk staff and not well-integrated into wider agency change-management processes.</p>	<p>Clear PIA process exists which is well-integrated into other risk assessment and change-management processes and connected to the agency's values.</p> <p>Preliminary risk assessments are routinely undertaken to assess whether or not a PIA is required.</p> <p>PIAs are completed by relevant change manager or project manager in collaboration with privacy and risk staff.</p> <p>PIAs are independently reviewed when appropriate.</p>	<p>PIA process is engaging and user-friendly. Tools and interactive templates are used to encourage involvement in development of the PIA by business owners.</p> <p>Privacy by Design principles are well understood and applied consistently across the agency.</p>

<sup>8</sup> Does not comply with the Code.

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>14. Dealing with Suppliers</b>	Limited or no assessment of third party privacy policies, practices or systems is undertaken.	<p>Some assessment is undertaken but agency approach is inconsistent and may vary between business units.</p> <p>Third party contracts include a confidentiality clause and standard privacy terms.</p>	<p>A documented and clear assessment process exists and is applied consistently where a third party may have access to personal information.</p> <p>Third parties are only engaged if their privacy practices are equivalent to the agency's or any gaps are mitigated by contractual controls.</p> <p>Contractual terms relating to privacy are supported by documented operational processes between the parties (for example on incident management and escalation processes).</p>	<p>The assessment process is well-developed and varies depending on the sensitivity of the personal information involved.</p> <p>Third party contracts include tailored privacy clauses to reflect the specific privacy risks involved.</p> <p>Third party assessment processes are continuously improved to ensure that emerging risks are mitigated in future contracts.</p> <p>Privacy audits of third parties are regularly undertaken to ensure they are meeting their contractual requirements, for example, by way of site visits.</p>

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>15. Access &amp; Correction*</b>	<p>No processes exist to ensure that an individual can request access to, or correction of, their personal information.</p> <p>No clear understanding by staff of individual rights of access and correction and how to balance privacy rights and FOI obligations.</p> <p>Rights often viewed negatively by the agency (<i>'it's our information, they can't see it'</i>).</p> <p>Limited understanding of information holdings means individual unlikely to receive complete response.</p> <p>Privacy Act response timeframe frequently exceeded.<sup>9</sup></p>	<p>Some documented processes exist but these are not fully known or consistently applied.</p> <p>All requests tend to be escalated to the Privacy Officer rather than applying a risk based approach which empowers other staff to respond to requests.</p> <p>Understanding of information holdings means individual is likely to receive complete response.</p> <p>Request handling and response is legalistic and compliance-focused.</p> <p>Privacy Act response timeframe occasionally exceeded due to resource limitations of privacy officer.</p>	<p>Clearly documented processes exist that are consistently applied.</p> <p>Strong understanding by staff of rights and processes across the agency. Privacy Officer acts as a central contact on privacy matters within the agency, however responses can be decentralised where appropriate.</p> <p>Request handling open, collaborative and customer-focused.</p> <p>Privacy Act response timeframe rarely exceeded.</p>	<p>Access and correction rights are viewed as an opportunity to engage with the public and show openness and transparency.</p> <p>Innovative approaches are taken to enabling access and correction, including the use of self-service portals.</p>

<sup>9</sup> May not comply with the APPs.

*Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.*

Attribute	Initial	Developing	Defined	Leader
<b>16. Complaints &amp; Enquiries</b>	<p>Staff are unaware of how to identify or manage a privacy complaint or enquiry.</p> <p>It is not clear to the public where to make a complaint or ask a question about privacy.</p> <p>Response to complaint or enquiry will depend entirely on the staff member who receives it.</p>	<p>Some staff are able to identify and manage a privacy complaint or enquiry.</p> <p>There is a general channel for the public to engage with the agency and this can be used for privacy complaints and enquiries (e.g. 'Contact us' web-form).</p> <p>Escalation process varies depending on business unit but there is an overreliance on the Privacy Officer to respond directly to complaints and enquiries.</p> <p>Limited use is made of complaints and enquiry data to improve privacy practice.</p>	<p>All business units who have contact with the public are enabled and empowered to handle privacy complaints and enquiries and know when escalation to the Privacy Officer is appropriate.</p> <p>The public has access to a specific privacy contact channel and staff with the knowledge and skills to respond meaningfully to a privacy complaint or enquiry.</p> <p>Good use is made of complaints and enquiry data to improve privacy practice.</p>	<p>Innovative approaches are taken to ensuring that the public has a clear and easy path to make privacy complaints or enquiries.</p> <p>FAQs or other interactive online tools are used to ensure that the public can access answers to common privacy questions or concerns and the agency improves these resources regularly.</p> <p>Complaints data is recognised as a valuable source of insights about public perception and concern and privacy weaknesses or issues.</p>

#### 4. Risk and assurance

This element measures how well-developed your risk and assurance processes are and how privacy fits into them. Your agency's risk management framework is a core element that will contribute to your agency's overall privacy maturity. This includes aspects of risk identification, assessment and treatment. A clear risk reporting process will enable senior leadership to make strategic decisions with adequate consideration given to the agency's privacy risk profile. Risk and assurance processes also provide a means for the agency to monitor and review the effectiveness of its privacy program.

*Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.*

Attribute	Initial	Developing	Defined	Leader
<b>17. Risk Identification &amp; Assessment</b>	No formal, structured or consistent process exists for identifying and assessing privacy risks.	Some documented privacy risk processes exist but they are reactive and compliance-focused.  There is limited integration with wider risk management frameworks.	Strong, clear and consistent processes exist for identifying and assessing privacy risks.  Privacy is integrated into agency's wider risk management framework.  Proactive steps are taken to identify privacy risks using all available sources of information (such as complaints, breach data, enquiries etc.).	Privacy risk identification is an accepted part of all business activity and management and staff perceive this as adding value.  Privacy is firmly integrated into agency's wider risk management function and always considered.  Innovative approaches are taken to identify and respond to privacy risks across the agency's functions.



*Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.*

Attribute	Initial	Developing	Defined	Leader
<b>18. Reporting &amp; Escalation</b>	Reporting is haphazard and largely limited to breaches and incidents.	<p>The agency's reporting lines and processes are defined and generally followed. Mechanisms ensure that senior management is routinely informed about privacy risks or issues.</p> <p>Thresholds for escalation of privacy risks, issues, incidents and complaints are becoming understood and adhered to by staff.</p>	<p>Privacy is monitored within the agency's broader risk and assurance framework, providing an integrated way of reporting on privacy risks, issues, incidents and complaints to senior management.</p> <p>The agency documents its compliance with privacy obligations, including keeping records on privacy process reviews, breaches and complaints and routinely reflects on ways to improve its processes.</p> <p>The agency's PIAs, privacy management plans and reviews of internal processes are endorsed by the agency's privacy champion.</p>	<p>Reporting to senior management extends beyond risks, issues and incidents and complaints to lessons learned, continuous improvement activities and innovation.</p> <p>The agency is open and transparent with the public about its reporting and escalation practices, procedures and systems, for example, by responding meaningfully when asked about them or including them in FAQs.</p>

*Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.*

Attribute	Initial	Developing	Defined	Leader
<b>19. Assurance Model</b>	Ad hoc assurance activities occur in response to breaches or incidents. There is no assurance in respect of the agency's privacy management plan.	<p>Some assurance activities occur in respect of the privacy management plan, processes and controls and in response to breaches or incidents. For example, the 'three lines of defence' model has been adopted for specific risks such as incident management. Under this model:</p> <ul style="list-style-type: none"> <li>• <b>First line</b> - privacy controls are implemented in response to breaches or incidents.</li> <li>• <b>Second line</b> - the Privacy Officer has oversight over breaches or incidents and controls that are adopted.</li> <li>• <b>Third line</b> - internal audit staff conduct assurance activities to ensure that controls are being effected properly.</li> </ul>	<p>Well-developed assurance activities occur in respect of the privacy management plan, processes and controls and other identified risks, or proactively because of other risk identification activities.</p> <p>A defined 'three lines of defence' model is in place, with strong privacy officer involvement:</p> <ul style="list-style-type: none"> <li>• <b>First line</b> - operational privacy risks are identified and recorded in risk register and control activities are documented.</li> <li>• <b>Second line</b> - the Privacy Officer collaborates with information security, data governance and risk functions to provide oversight of privacy risk management.</li> <li>• <b>Third line</b> - internal audit (or independent assessors) conduct regular privacy-related assurance activities.</li> </ul>	<p>Assurance activities routinely drive improvement and innovation in privacy management.</p> <p>The 'three lines of defence' model means that:</p> <ul style="list-style-type: none"> <li>• <b>First line</b> - the agency's business functions take ownership of ensuring that privacy controls are in place.</li> <li>• <b>Second line</b> - the Privacy Officer collaborates with information security, data governance and risk functions to identify opportunities for best practice and continuous improvement.</li> <li>• <b>Third line</b> - independent assurance is regularly sought to ensure not only that the agency is fully compliant but that best practice is achieved and demonstrated.</li> </ul>

## 5. Data Breach Response

This element measures your agency's readiness to identify and handle a data breach and to ensure that the requirements of the [Notifiable Data Breach \(NDB\) scheme](#) are understood and followed. An agency's ability to properly manage a data breach is reliant on the existence of a strong privacy culture (staff need to know what a data breach looks like and feel safe to speak up about it) and risk and assurance processes that are capable of recognising breaches and ensuring that steps are taken to prevent recurrences. Effective data breach responses are ultimately about protecting individuals from harm and this element therefore also considers how capable your agency is to engage with individuals with sensitivity and compassion.

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
<b>20. Data Breach Response Plan</b>	<p>No structured approach to data breach response exists.</p> <p>Staff are unlikely to recognise a data breach and are unlikely to speak up about breaches due to potential consequences for them.<sup>10</sup></p>	<p>A basic data breach response plan in place that reflects the OAIC's recommended steps (Contain, Assess, Notify, Prevent). Plan is not consistently followed but becoming better known.</p> <p>Staff are generally aware of how to recognise a data breach, and are likely to speak up about breaches.</p> <p>Decision making in breach response is largely reliant on the Privacy Officer.</p>	<p>There is a well-defined plan in place with clear and documented roles and escalation paths.</p> <p>Staff are aware of how to recognise a data breach and are likely to speak up. There is a strong culture of openness and trust that results in staff confidence and honesty.</p> <p>Accountabilities for data breach responses and decision making are spread across the agency.</p> <p>Process is integrated with other critical business functions, including information security, communications and risk and assurance.</p>	<p>The agency's response plan is regularly tested using breach simulations and other assurance activities to ensure it is continuously improved. Innovative approaches are adopted.</p> <p>The agency is open about its data breach experiences and engages with the public and stakeholders about them.</p> <p>The agency willingly assists other agencies to lift their practices by sharing its data breach experiences and plans.</p>

<sup>10</sup> May not comply with Privacy Act (Notifiable Data Breach scheme).

**Maturity levels are cumulative – the criteria for each level must be met before moving to the next level.**

Attribute	Initial	Developing	Defined	Leader
			Effective processes exist to ensure lessons learned and prevention measures are documented and implemented.	
<b>21. Data Breach Notification*</b>	<p>Data breach notification is viewed negatively and is unlikely to occur.<sup>11</sup></p> <p>There is no process in place to evaluate the breach and assess whether notification is necessary or desirable. Little to no knowledge or understanding of breach notification requirements, such as notification thresholds.</p> <p>Breach and notification risk is viewed only as a harm to the agency. Little to no consideration is given to how affected individuals may be harmed.</p>	<p>Data breach notification only occurs where required under legislation.</p> <p>Processes are developing to evaluate a breach and assess whether notification is required.</p> <p>Determining whether to notify is driven by Privacy Officer with frequent opposition from other agency stakeholders.</p> <p>The agency is focused on preventing harm to individuals and takes proactive steps to assist affected individuals (for example, directing them to support and resources inside and outside the agency).</p>	Clear processes are in place to evaluate breaches and assess whether notification is necessary or desirable. Other stakeholders understand the obligations and benefits of notification.	<p>Data breach notification is viewed as an opportunity to demonstrate trust and transparency.</p> <p>Communications are individualised and appropriate and the agency follows up with the affected individuals to ensure that mitigation steps have been successful.</p>

<sup>11</sup> May not comply with the Privacy Act (Notifiable Data Breach scheme).