Australian Government
Office of the Australian Information Commissioner

Privacy Management Plan

Office of the Australian Information Commissioner

1 July 2024 to 30 June 2025

Background

What is a Privacy Management Plan?

All Australian Government Agencies are required to have a Privacy Management Plan (PMP) under the Australian Government Agencies Privacy Code. The PMP identifies specific, measurable privacy goals and targets and sets out how an agency, including the Office of the Australian Information Commissioner (OAIC) will meet its compliance obligations under APP 1.2. The OAIC must measure and document its performance against its privacy management plan at least annually.

Before developing a PMP, every agency will need to understand the current state of their privacy practices. The OAIC has built on previous PMPs and used the OAIC's *Interactive PMP Explained* resource to help identify opportunities to improve maturity.

What are the next steps?

This PMP describes the actions that the OAIC must take in order to meet its privacy compliance obligations and maturity targets for the year following the PMP's commencement date 1 July 2024. The OAIC PMP FY 24/25 builds on actions identified in previous PMPs to improve maturity levels and record how it has done so. The PMP Steering Committee has a focus on innovative approaches to delivering PMP Compliance Activities and as part of considerations for subsequent PMPs.

About this PMP

Agency name	Office of the Australian Information Commissioner
PMP commencement date	Monday, 1 July 2024
PMP end date	Following commencement, this PMP will operate until Monday, 30 June 2025.
Recommended review period	Tuesday, 1 April 2025 to Monday, 30 June 2025

Privacy risk profile

In the course of preparing this PMP, the OAIC has considered various matters relevant to its privacy risk profile. The details of these considerations are provided below for reference.

Privacy risk profile rationale

The OAIC has determined that it has a high privacy risk profile, primarily because:

a) The OAIC has regulatory oversight of entities under the Privacy Act in respect of their handling of personal information;

b) The OAIC has a number of functions and powers under the Privacy Act, the FOI Act and other laws in relation to the conducting of investigations, the handling of complaints, the reviewing of decisions made under the FOI Act, monitoring agency administration and advising the public, organisations and agencies and its other stakeholders in the course of which it collects and handles personal information. Whilst the volume of records it holds is relatively low, complainant information may be 'sensitive information' under the Privacy Act, or by its nature be considered sensitive to the individuals and respondents involved. The information will sometimes relate to vulnerable members of the community; and

c) The OAIC relies on the trust of the community to fulfil its privacy and FOI functions. Individuals must be willing to freely provide their personal information to the OAIC so that it can effectively handle privacy and FOI complaints and investigations, and undertake IC review. Community confidence in the OAIC’s findings is an important aspect of a functioning regulatory system.

Current state

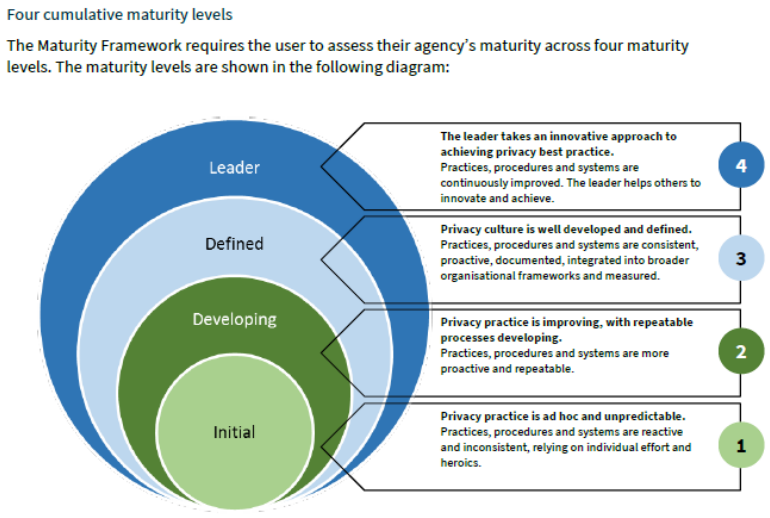
Privacy maturity assessment outcomes

This PMP has been prepared using an assessment of the OAIC's privacy maturity, the results of which are recorded in the table below. An asterisk (*) next to an attribute name means that it is a 'compliance attribute' and that the OAIC must have a minimum maturity level of 'Developing' to comply with the Privacy Act or the Code.

The OAIC's overall rating is currently at 'defined' maturity level. The OAIC privacy management maturity level of Defined is based on a Privacy Program Maturity Assessment Framework outlined in the Interactive Privacy Management Plan Explained resource.

Defined maturity level

Defined maturity level means Privacy culture is well developed and defined. Practices, procedures and systems are consistent, proactive, documented, integrated into broader organisational frameworks and measured. The diagram below explains the four cumulative maturity levels obtained from the 'Interactive PMP explained' Guidance (D2022/014055, page 25).



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:

4 **The leader takes an innovative approach to achieving privacy best practice.** Practices, procedures and systems are continuously improved. The leader helps others to innovate and achieve.

3 **Privacy culture is well developed and defined.** Practices, procedures and systems are consistent, proactive, documented, integrated into broader organisational frameworks and measured.

2 **Privacy practice is improving, with repeatable processes developing.** Practices, procedures and systems are more proactive and repeatable.

1 **Privacy practice is ad hoc and unpredictable.** Practices, procedures and systems are reactive and inconsistent, relying on individual effort and heroics.

The compliance activities identified below outline steps the OAIC needs to take in order to reach the appropriate privacy maturity target level of Defined or Leader.

Governance & Culture				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
Privacy Champion*	**Leader**	**Leader**	The OAIC meets the criteria for the Leader maturity level. As the designated Privacy Champion, the Deputy Commissioner has been charged by the OAIC Executive with holding relevant responsibilities for privacy management under the Privacy Code and these are incorporated into their performance management agreement. In this capacity, the Deputy Commissioner has the mandate to speak publicly on privacy and information matters, as well as driving improvements to, and being responsible for, the agency's privacy culture. The OAIC Privacy Champion position role and description is published on the OAIC website.	The Privacy Champion will continue public engagements on privacy and information matters and to drive improvements for the OAIC's privacy culture. The roles and responsibilities of the Privacy Champion, Chief Privacy Officer and Privacy Officers will be reviewed annually to ensure it remains relevant and effective.
Privacy Values	**Leader**	**Leader**	The OAIC meets the criteria for the Leader maturity level. The OAIC publicises its values which promote a culture of valuing and protecting personal information. The OAIC runs an annual Privacy Awareness Week (PAW) campaign to promote the importance of protecting personal information and privacy values. This value is demonstrated in every aspect of the OAIC's functions and activities.	The OAIC will continue to promote privacy values through PAW, OAIC communication channels such as newsletters and social media platforms, and through the delivery of its functions and activities.

Privacy Officer*	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. The OAIC Privacy Officer has established practices, procedures and systems that correlate with the OAIC's data governance, customer engagement and other transformation functions. These practice and procedures are documented and integrated into broader organisational frameworks. The Privacy Officer is encouraged to innovate practices, procedures and systems, ensuring privacy is at the forefront of consideration for all OAIC initiatives. The Leader maturity level for this attribute requires a Privacy Officer to willingly assist other agencies by sharing information and learnings about their role as a privacy officer. In its regulatory space, the OAIC has developed and disseminated a suite of guidance material to government agencies, including their Privacy Officers. The OAIC also shares information about the role of the Privacy Officer under the Privacy Code by the sharing of various resources through the Privacy Professionals Network and the Privacy Officer networks.	The OAIC Privacy Officers will continue to regularly review privacy practice, procedures and systems through broader integrated organisational frameworks. OAIC Privacy Officers will continue to share information and learnings 1-2 times a year through the OAIC privacy and data champion networks.

Management & Accountability	**Leader**	**Leader**	The OAIC meets the criteria for the Leader maturity level. The measurement of the OAIC's performance and continuous improvement initiatives are undertaken and reported to the Executive regularly. The roles and accountabilities for privacy compliance are documented and promoted across the agency regularly. The OAIC publishes the Executive structure. Documents relating to who holds accountability for privacy at the OAIC are published on our website. The OAIC has also published documents on management and accountability practices in its website through various documents, including via delegation instruments, its privacy policies and annual reports. The OAIC conducts annual reviews of its privacy practices, procedures and systems, including its privacy policy and notices, records management policies, privacy risks and service charter, as part of its Controlled Documents Register framework, and strives for continuous improvement.	The Chief Privacy Officer and Privacy Officers will continue to review OAIC’s performance through the OAIC PMP and report to the Executive regarding its progress on a regular basis. The regular review of OAIC key policy and procedure documents are embedded in the OAIC’s Controlled Documents Register framework.
Awareness	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. OAIC has established the PMP Steering Committee comprised of membership across all OAIC Branches to carry out PMP compliance activities and establish, review and disseminate relevant internal policies and procedures. This ensures all Branches are aware of their privacy responsibilities and obligations. Staff view privacy as an enabler and know how to apply OAIC privacy policies and expectations to emerging issues. The OAIC shares substantial privacy awareness resources though its website and works with agencies	The OAIC continues to work with various sections across the Office to develop and share resources internally and externally for various sectors; e.g., the OAIC has resources relating to individuals, consumers, government agencies, businesses, health and credit sectors etc.

			and organisations, as well as public and private sector groups, to develop resources which are relevant to the needs of specific stakeholders. The OAIC works together with business and industry sectors and Government Agencies to develop sectoral resources which meet the needs of the sector, as well as the specific needs of each agency.	The OAIC Privacy Officer will regularly share resources, advice and/or learnings regularly (at least annually).
Element score (average of attribute scores)			**3.4 / 4 (Defined)**	

Privacy Strategy				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
Privacy Management Plan*	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. The OAIC publishes its Privacy Management Plan (PMP) and its progress against it internally and externally. The OAIC addresses the protection of personal information throughout the information lifecycle. It includes actions to improve maturity outcomes and assigns responsibility and target completion dates for each action. Progress as against each action is tracked and reported to the OAIC Executive. The OAIC's Privacy Management Plan 2024-2025 will be published on the OAIC website. To achieve Leader maturity level for this attribute requires the OAIC to publish its PMP and its progress against it. The OAIC's focus on innovation should be apparent in its PMP.	The OAIC will continue to share its progress internally and externally through by publishing its annual PMP and PMP Summary at the end of each reporting period.
Inventory of Personal Information*	**Defined**	**Defined**	The OAIC meets the criteria for the Defined maturity level. The OAIC has documented its personal information holdings in a Personal Information Inventory (PII) in the context of broader organisational goals and priorities. The OAIC has an awareness of all data flows in and out of the agency. The OAIC has implemented an annual review process to monitor and map changes to its personal information holdings. The maturity framework specifies that to achieve a	**Compliance Activity 1** The OAIC will continue to review its PII annually. The process is embedded in the Controlled Documents Framework for annual review. The PMP Steering Committee will consider whether the OAIC could

			Leader maturity level, the OAIC would need to consider publishing and sharing its personal information inventory where appropriate, and must use data-driven decision-making to identify opportunities and risks related to its personal information holdings. The Leader maturity level for this attribute requires an innovative and sophisticated approach to the development of the IT systems which house the records of personal information holdings. The OAIC would also be required to proactively publish its record where appropriate and to share insights and advice with other government agencies. The OAIC's personal information holdings are limited in scope and volume, and not easily suited to data-driven decision-making. Accordingly, the OAIC has determined that a Defined level of maturity is appropriate for 2024-2025.	have a more innovative approach to house the record of personal information holdings.

Data Quality Processes*	**Leader**	**Leader**	The OAIC meets the criteria for the Leader maturity level. The OAIC staff are aware of the importance and value of keeping personal information relevant and up to date, and take action to correct and update records where appropriate. The OAIC promotes data quality practices across the public and private sectors through resources published on its website. The OAIC regularly investigates and takes opportunities to enhance its processes for ensuring the quality of personal information. The OAIC has strict retention and destruction policies which complement data quality processes and audits are conducted on an ongoing basis. See the OAIC's Disposal Authority for more information.	The OAIC will continue to review and conduct ongoing audits and to explore opportunities to innovate its processes for ensuring quality of personal information.

Information Security Processes	**Defined**	**Defined**	The OAIC meets the criteria for the Defined maturity level. It has an established information-security aware culture, reinforced by scheduled audits. Staff have access to guidance materials and training to ensure an understanding of the commonalities and differences between privacy and security and an awareness of relevant privacy and security policies and processes. The Leader maturity level for this attribute requires an agency to assist other agencies by sharing its experiences and insights to encourage collaboration between privacy, information security and other functions. The OAIC's information systems are managed under a shared services arrangement, and while the OAIC does share its knowledge in relation to privacy and information security with other agencies through its regulatory role, it is not in a position to proactively collaborate in depth in respect of its insights into its own information security processes. Accordingly, the OAIC has determined that a Defined level of maturity is appropriate.	The OAIC will continue to promote information security and to review related guidance, policy and processes.
Element score (average of attribute scores)			**3.3 / 4 (Defined)**	

Privacy Processes				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
External Privacy Policy & Notices*	**Leader**	**Leader**	The OAIC meets the criteria for the Leader maturity level. Privacy messaging is viewed as an opportunity to build trust and engage the public. The OAIC holds the annual Privacy Awareness Week and uses the opportunity to delivery privacy messaging to the public using infographics, animation, games, videos, webinars and other forms of technology to increase user experience. The OAIC privacy policy, privacy policy summary and human resources privacy policy are publicly available on the OAIC website. They are reviewed and updated at least annually. The OAIC has adopted a tiered privacy policy, written in plain English and with a Flesch Kincaid Reading Ease Score of 6 (suitable for 11-12 year olds).	The OAIC will continue to review and update its Privacy Policies and issue notices on relevant updates.

Internal Policies & Procedures	**Leader**	**Leader**	The OAIC meets the criteria for the Leader maturity level. Staff and management proactively contribute to improving internal privacy policies and procedures. Internal privacy policies and procedures are an integral part of the way that the agency functions. Internal privacy policies and procedures are proactively reviewed and updated to ensure that they encourage privacy best-practice and drive culture and behaviour. The documents are reviewed periodically as part of a Controlled Document Register framework. The documents are disseminated to all staff when updated and are available for all staff to access. The OAIC distributes and sends staff reminders about new and updated privacy policies and procedures within the agency on a regular basis as part of its internal communications processes.	The OAIC will continue to review internal policies and procedures on a regular basis and circulate updates to all staff.
Privacy Training*	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. The OAIC Learning and Development strategy sets out that staff receive induction training and annual refresher training. Personnel who directly engage with individuals or handle personal information in their roles receive more targeted training, though regard is given to the fact that staff handling complaints have a very high level of awareness about appropriate privacy practices resulting from their work. Staff completion rates and understanding of privacy are monitored. All staff are encouraged to participate in regular discussions on emerging privacy issues. The OAIC aims to move to a Leader maturity level by continuing to explore innovative ways to deliver training to staff using innovative approaches (e.g., online	The OAIC will continue to deliver relevant training to new and existing staff training. The PMP Steering Committee will continue to look at innovative ways to deliver relevant privacy training regularly (at least annually) to all staff.

			training modules, driven in part by the OAIC's move to a hybrid working environment).	
Privacy Impact Assessments*	**Leader**	**Leader**	The OAIC meets the criteria for the Leader maturity level. The OAIC has developed internal PIA guidance that is engaging and user-friendly. The internal guidance includes links to external-facing guidance and resources, including tools and templates, on the OAIC website. OAIC routinely carries out Privacy Threshold Assessments to determine whether full PIAs are required for initiatives which involve either handling of new kinds of personal information or new ways of handling existing personal information, and risks that are identified are reported to the OAIC Executive with recommended controls. If risks are high, full PIAs are undertaken. The OAIC follows the methodology published on its website. PIAs are independently reviewed when appropriate. Privacy by design principles are applied consistently	The OAIC will continue to conduct Privacy Threshold Assessments and Privacy Impact Assessments and publish related Registers on the OAIC website. We will also continue to review related internal documents regularly to ensure it remains useful and effective.

			across the OAIC with express consideration to privacy impacts embedded in project and Executive brief templates.	

Dealing with Suppliers	**Defined**	**Defined**	The OAIC meets the criteria for the Defined maturity level. The OAIC is developing a documented process for assessing and managing risks associated with suppliers that may hold or access personal information. The OAIC currently mitigates risks through contractual terms with suppliers and supporting operational processes (for example on incident management and escalation processes). ICT and legal suppliers sign an NDA before accessing personal information, and where appropriate, may undertake in-house privacy induction training. The Department of Education Skills and Employment (DESE), now renamed to the Department of Employment and Workplace Relations (DEWR), performed certain administrative functions on behalf of the OAIC under a shared services arrangement as of June 2023. To achieve Leader maturity level third party contracts should include tailored privacy clauses to reflect the specific privacy risks involved. Third party assessment processes are continuously improved to ensure that emerging risks are mitigated in future contracts. Privacy audits of third parties should be regularly undertaken to ensure contractual requirements are met. The OAIC can also work towards Leader level by centralising and further documenting privacy risk management processes for on-boarding and off-boarding of suppliers.	The OAIC will continue to manage risks associated with suppliers through PTA and PIA processes. The OAIC currently mitigates risks through contractual terms with suppliers and supporting operational processes (for example on incident management and escalation processes). ICT and legal suppliers sign an NDA before accessing personal information, and where appropriate, may undertake in-house privacy induction training. **Compliance Activity 2** Develop a consolidated documented process for assessing and managing risks associated with suppliers that may hold or access personal information.

Access & Correction*	**Defined**	**Leader**	The OAIC meets the criteria for Defined maturity level. The OAIC routinely gives individuals access to their personal information via different mechanisms. Individuals may seek access to their personal information in the course of a complaint, and this is dealt with informally under administrative access. Formal access and correction requests may be made to the OAIC under APP 12 and APP 13 of the Privacy Act, and the OAIC is bound by the Act to follow the processes under those provisions. The OAIC is in the process of finalising internal policies in relation to the processing of APP 12 and 13 requests. The OAIC strives to meet its regulatory timeframes. It consciously undertakes to be responsive, open and transparent in its dealings with access and correction requests. To achieve Leader level, the OAIC should take innovative approaches to enabling access and correction, including the use of self-service portals.	**Compliance Activity 3** The OAIC will finalise internal guidance for staff on administrative access and APP 12 request. The PMP Steering Committee will consider whether innovative approaches in conjunction such as the introduction of self-service portals would be appropriate for OAIC use.

Complaints & Enquiries	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. The OAIC is using innovative approaches to identify ways to better manage the complaints process and to make good use of complaints and enquiry data by exploring digital automated reporting capabilities. Complaints made to the OAIC about its own conduct in relation to personal information are received and managed by the OAIC's legal team. The legal team incorporates, where appropriate, established processes under the OAIC's Dispute Resolution regulatory function to handle privacy complaints made against it. OAIC has published its overarching policy and process for complaints about OAIC employees or contractors on its website to ensure the public is aware of the OAIC's complaints and handling processes. The Leader maturity level requires the OAIC use FAQs or other online tools to ensure public can access answers to common privacy questions or concerns. Complaints data should also be recognised as a valuable source of insight about public perception, concern and privacy weaknesses or issues.	**Compliance Activity 4** The PMP Steering Committee will review the OAIC website, following the completion of website migration, to ensure the procedure and processes to make complaints about the OAIC's handling of individual personal information is easily understood and accessible. The PMP Steering Committee will consider whether resources such as FAQs or other interactive online tools could be used to assist the public to access answers to privacy questions or concerns about the OAIC.
Element score (average of attribute scores)			**3.4 / 4 (Defined)**	

Risk & Assurance				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
Risk Identification & Assessment	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. The OAIC has strong, clear and consistent processes to identify and assess privacy risks as part of its PIA and risk management policies and procedures. All initiatives involving new ways of handling personal information are assessed for privacy risk as part of the PTA and PIA processes and are reported to the Executive and Chief Privacy Officer in a timely manner. Privacy risk is acknowledged as part of all business activity and risk management strategies are used to manage perceived or actual risks. Privacy is firmly integrated into the agency's wider risk management function and always considered. The OAIC raises awareness of privacy risk management processes amongst staff, ensuring that privacy risks are identified in 'business as usual' activities (as opposed to new initiatives) through regular internal communications. Identified risks are captured within existing risk review processes for trends and learnings which can drive continuous improvement. The OAIC can target the Leader maturity level by considering innovative approaches to identify and respond to privacy risks across the OAIC's functions.	The OAIC will continue to conduct Privacy Threshold Assessments and Privacy Impact Assessments and review privacy risk on a regular basis. The OAIC is in the process of reviewing and considering innovative approaches to identify and respond to privacy risks across the OAIC functions. The PMP Steering Committee will consider and incorporate any findings in subsequent PMPs.

Reporting & Escalation	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. The OAIC documents its compliance with privacy obligations, including keeping records and data. The OAIC's Executive team also receives scheduled reports on the agency's operational metrics. As part of this reporting process, the Executive team considers recommended controls and monitors their effective implementation. The OAIC's PIAs, PMPs and review of internal processes are endorsed by the agency's Privacy Champion. The OAIC continues to review and update its risk management and governance frameworks and publish these on our intranet and/or website. The OAIC may target the Leader maturity level by implementing a more detailed reporting process which builds on existing reporting of risks, issues and incidents and complaints to add lessons learned, continuous improvement activities and innovation. To achieve this maturity level, the OAIC should also be open and transparent with the public about its reporting and escalation practices, procedures and systems, e.g., through the publication of more detailed information about the OAIC privacy processes and procedures through information access regimes or FAQs.	The OAIC will continue to report to the OAIC Executive regarding risks, issues, incidents and focus on continuous improvement activities and innovation. The OAIC will also continue to remain open and transparent with the public by regularly reviewing OAIC reporting and escalation practices, procedures and systems and publishing relevant updates. **Compliance Activity 5** The PMP Steering Committee will review how the OAIC deals with privacy complaints made to the OAIC and identify gaps in our privacy complaint handling processes.

Assurance Model	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. The OAIC has adopted an informal 'three lines of defence' risk and assurance model whereby: 1) Personnel in the OAIC's Branches have primary responsibility for identifying and escalating privacy issues, including to the Privacy Officers/CPO; 2) The Privacy Officers/CPO provides guidance, collaborates with information security, data governance and risk functions to identify opportunities and best practice and continuous improvement; and 3) The OAIC regularly engages third parties to provide independent assurance that the OAIC has complied with its obligations. The OAIC relies on the roles played by its three lines of defence to drive improvements and innovation in the OAIC's information handling practices. The CPO will consider trends in escalated privacy issues and seek input from third parties to identify improvement activities for the subsequent PMPs. The OAIC can target Leader level maturity by obtaining independent assurance to ensure that best practice is achieved and demonstrated.	**Compliance Activity 6** OAIC will periodically (e.g., annually) consider trends in reporting of privacy risks, escalated privacy issues and input from third parties to identify improvement activities for subsequent PMPs. Consider engaging external third party to conduct audits and help identify further areas for improvement for subsequent PMPs.
Element score (average of attribute scores)			**3 / 4 (Defined)**	

Data Breach Response				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
Data Breach Response Plan	**Defined**	**Leader**	The OAIC meets the criteria for the Defined maturity level. The OAIC has a well-defined Data Breach Response Plan (DBRP) with clear and documented roles and escalation paths which it has published on its website. The DBRP has been integrated with other business critical functions including information technology and physical security. The DBRP is accessible to all staff and agency-wide emails have been used to build awareness of how to recognise a data breach and apply the plan. The DBRP is to be tested every 12 months via simulation. The OAIC will test the plan annually and will implement lessons learned and prevention measures as appropriate as part of the process. A Leader maturity level requires the OAIC to willingly assist other agencies lift their practices by sharing its data breach experiences and plans. The OAIC has published its Data Breach Response Plan and will consider how it can share its learnings to help other agencies lift their practices.	The OAIC will continue to review and test its Data Breach Response Plan and share updates to the Data Breach Response Plan. The PMP Steering Committee will consider how it can share its data breaches experiences.

Data Breach Notification*	**Leader**	**Leader**	The OAIC meets the criteria for the Leader maturity level. The OAIC's DBRP sets out the relevant test for determining whether notification is required under the Notifiable Data Breaches Scheme and if notification is not required, whether it should be voluntarily undertaken. The OAIC understands the need to prevent serious harm to individuals and takes proactive steps to assist affected individuals (for example, directing them to support and resources). The OAIC undertakes to be open and transparent in its breach management and notification practices, viewing data breach notification as an opportunity to demonstrate trust and transparency. The OAIC is committed to regularly discussing its DBRP at Branch meetings, incorporating data breach notification processes and procedure into its induction training and including reminders about escalation of breaches into its annual awareness program. These activities are aimed at further embedding a culture that recognises the importance of maintaining trust in the case of a data breach, and the importance of appropriately individualised communications and remedial actions.	
Element score (average of attribute scores)			**3.5 / 4 (Defined)**	

Average of element scores	**3.4 / 4**	
Overall privacy maturity level	**3 / 4 (Defined)**	

Goals for improvement

The privacy goals and targets in this section are based on the agency's privacy maturity assessment outcomes above.

Maturity Improvement Actions

The table below sets out actions which the agency plans to achieve in order to improve its privacy maturity. Any uncompleted actions from previous PMPs which are still relevant should also be documented in this section to ensure that they form part of the agency's next PMP.

Element/Attribute	Compliance Action	Responsible sections	Due date	Required resources/related documents and comments
Privacy Strategy / Inventory of Personal Information	1. PMP Steering Committee to review OAIC Personal Information Inventory (PII) holdings, identify privacy risks associated with OAIC PII and adopt strategies to address risks.	Chief Privacy Officer/PMP Steering Committee	Q1	This activity has been carried over from PMP FY 23/24 - compliance activity 1. PMP Steering Committee to identify whether PII holdings can be disposed of in accordance with the OAIC Records Authority. Timely destruction of documents in accordance with the OAIC records authority has been flagged as an area of weakness. Awareness of this must be raised this FY, and improvement activities

				identified and undertaken. As part of the process, consider innovative ways in which the OAIC can manage personal information and PII processes.
Privacy Processes/Dealing with Suppliers	2. Develop a consolidated documented process for assessing and managing risks associated with suppliers that may hold or access personal information.	Legal Services, Chief Privacy Officer in consultation with Privacy Champion	Q4	This activity has been carried over from PMP FY 23/24 under compliance activity 2. The OAIC currently mitigates risks through contractual terms with suppliers and supporting operational processes (for example on incident management and escalation processes). ICT and legal suppliers sign a NDA before accessing personal information, and where appropriate, may undertake in-house privacy induction training.

Privacy Processes/ Access and Correction	3. Finalisation of the Guidance for staff on administrative access and APP 12 requests. The PMP Steering Committee will consider whether innovative approaches in conjunction such as the introduction of self-service portals would be appropriate for OAIC use.	Legal Services Team	Q1	This activity has been completed under PMP FY 23/24 - compliance activity 3. Review of the current guidance for staff to ensure that current approaches would still be appropriate.
Privacy Processes / Complaints & Enquiries	4. Review the information on the website to ensure complaints about the OAIC's handling of individual's personal information (as an agency) is easily understood, and the public is easily able to lodge a complaint to the OAIC in respect of its information handling practices, e.g., how to contact us, developing FAQs.	Chief Privacy Officer/ Legal Services/ IMPS	Q4	This activity has been carried over from PMP FY 23/24 under compliance activity 4.
Risk & Assurance / Reporting & Escalation	5. Review how the OAIC has dealt with privacy complaints made to the OAIC to identify any gaps in privacy complaint handling procedure and processes.	Chief Privacy Officer/ Legal Services/ PMP Steering Committee	Q3	This activity has been carried over from PMP FY 23/24 under compliance activity 5.

Risk and Assurance/ Assurance Model	6. Privacy Officer will periodically (e.g., annually) consider trends in reporting of privacy risks (currently dealt with through the OAIC Data Breach Incident Log and privacy complaints against the OAIC), escalated privacy issues and input from third parties to identify improvement activities for subsequent PMPs to improve risk detection and risk resilience (containment and mitigation) within the OAIC. The CPO/Legal Services will engage with Privacy DR through to ensure learnings are incorporated into PMP considerations to help identify further areas for improvement for subsequent PMPs.	Chief Privacy Officer/Legal Services/PMP Steering Committee/Privacy DR	Q4	This activity has been carried over from PMP FY 23/24 - compliance activity 6. It is noted that Privacy DR is developing a process to ensure best privacy practices arising from privacy DR decisions or policy approaches are captured and embedded in OAIC regulatory activity. Improvements in subsequent PMPs will be impacted by the outcome of the process.
Governance & Culture	7. Review and assess the current maturity levels of the OAIC through an independent assessor to ascertain the accuracy of current levels and how to address any variances.	Chief Privacy Officer in consultation with Privacy Champion, PMP Steering Committee.	Q4	This is a new activity to be discussed with the PMP Steering Committee.

Measure performance

It is expected that the OAIC will review this PMP during the time in which it is active in order to document progress against the actions described above.

The CPO will provide the OAIC Operations Committee with a fortnightly update to track progress.