information and privacy commission
new south wales

Follow-up Desktop Audit of Privacy Management Plans (PMP) Report

June 2023

Contents

Executive Summary

In December 2021, the Information and Privacy Commission (IPC) published the *Desktop Audit Privacy Management Plans (**PMP**) Report* (**2021 Report**) of universities, select councils and the government departments' compliance with the Privacy Management Plan (PMP) requirements under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act). The 2021 Report followed evidence given by the Privacy Commissioner to the NSW Parliament Cybersecurity Inquiry[1] relevant to observations about the currency of privacy management plans within regulated entities in NSW.

The 2021 Report provided a baseline measure of a sample of agencies' performance against three criteria against which their PMP was measured. Its findings generally observed that opportunity existed for agencies to take positive action to improve and elevate practices in relation to PMPs generally. In particular, the Privacy Commissioner noted that the value derived from a PMP was diminished if it was not maintained and lacked currency, especially against an environment of increasing digital transformation relied upon by agencies to undertake their functions and deliver services. After the 2021 Report, the IPC engaged extensively with entities captured by the report to support their compliance with the findings from the review and to support remediation action where required.

In summary, the outcomes from this follow-up review found for those agencies that were reviewed as part of the 2021 Report:

- 79% (23 agencies) that were reviewed in the 2021 Report had submitted a PMP to the IPC in 2022
- Of those 79%, 39% (9 agencies) were from the local government sector; 35% (8 from the university sector) and 26% (6 from the public sector)

In respect of the additional local government agencies included to this follow-up review the findings observed:

- 100% (10) of the local government sector that were reviewed had published their PMP to the agency website
- 70% (7) agencies made their PMPs easily locatable on their website on a dedicated privacy page
- 90% (9) agencies had a PMP that was dated earlier than 1 December 2020
- Of the 90% with a PMP dated 1 December 2020 or earlier, 33% (3) included published PMPs last updated in between the period 2019 – 2015
- 22% (2) were found to have a PMP from earlier than 2014 with at least one dating back to 2010.

The review of the extent to which agencies generally had been submitting their PMPs to the IPC as required[2] found:

- 18% (12) agencies submitted a PMP to the IPC for review in 2020
- 22% (15) agencies submitted a PMP to the IPC for review in 2021
- 60% (40) agencies submitted a PMP to the IPC for review in 2022.

The results demonstrate that while there was progress made in relation to the agencies that were subject of the 2021 Report, together with some improvement in the numbers of PMPs submitted to the IPC, the results in relation to the additional agencies included in this audit

[1] NSW Parliament, Report 52 – PC1 – Premier and Finance - Cyber security report at p27.

[2] Section 33(5) PPIP Act

continue to demonstrate gaps in the currency of the PMPs within agencies. Many of the recommendations made in the 2021 Report, had they been adopted by these agencies, would have likely produced a very different result and improved outcome. The IPC recognises that it has a positive role in assisting agencies to mature the level of compliance around a PMP, but it will also require positive leadership by senior officers within agencies to signal the importance, necessity, and support for currency around policies, practices and processes for the handling of personal/health information which are reflected in PMPs.

1. Background

The PPIP Act makes it a requirement that all agencies are to have a PMP[3]. In summary the PPIP Act requires that the PMP must include provisions relating to:

- the devising of policies and practices to ensure compliance by the agency with the PPIP Act or the *Health Records and Information Protection Privacy Act 2002* (HRIP Act)
- the dissemination of those policies and practices to persons within the agency
- the procedures that the agency proposes to provide in relation to internal review under Part 5 of the PPIP Act
- such other matters as considered relevant by the agency in relation to privacy and the protection of personal information held by the agency[4].

Agencies must provide a copy of their PMP to the Privacy Commissioner as soon as practicable after preparation or amendment[5].

A PMP ensures agencies have identified how the requirements of the PPIP Act and the HRIP Act apply to the personal and health information that they manage. It explains the agency's functions and activities and the main types of personal or health information that the agency deals with to carry out those functions and activities, together with its strategies to comply with the PPIP Act and HRIP Act. PMPs equip agency staff with the necessary knowledge and skills to manage personal and health information appropriately. As publicly available information, the PMP ensures that citizens interacting with the agency can be informed of:

- how to make a complaint or request an internal review if they consider that their privacy may have been breached
- how to request access to their personal or health information or an amendment of that information to ensure that it is accurate
- encourages the agency to be transparent and accountable in how it manages personal and health information.

In this way the PMP is a valuable resource that serves a dual purpose, for both agency staff and citizens.

In 2021 the Privacy Commissioner published her initial report on a review of agency PMP compliance. The 2021 Report made five recommendations for agencies and a further two recommendations for the IPC to take forward. Following the publication of the initial report, the IPC continued to engage with those agencies included within that report to support the adoption of the recommendations made, in particular with respect to the currency of PMPs. Of the recommendations made, one communicated the intention of the Privacy Commissioner

[3] Section 33(1) of the PPIP Act

[4] Section 33(2) of the PPIP Act

[5] Section 33(5) of the PPIP Act

to undertake a further follow-up audit 12 months after the 2021 Report. Agencies have therefore had notice of the Privacy Commissioner's intention since December 2021.

In conjunction with the follow-up audit, the desktop audit was expanded to consider an additional sample selection of local government councils as well as review the extent to which there had been any notable change in the number of PMPs submitted to the Privacy Commissioner following the 2021 Report.

Therefore, this review was broader than the scope of the previous review and examined and considered:

1. For agencies reviewed in the 2021 Report, whether a PMP for review had been submitted in 2022
2. For the additional agencies included to the review whether there was evidence of:
    - existence of a PMP on an agency website
    - the currency of the PMP, including whether the PMP has a review date of within the immediate past 12 months, and
    - where a PMP exists on an agency website and identifies as having been reviewed within the immediate past 12 months, whether the IPC's records demonstrate whether that PMP was submitted for review to the IPC.
3. The level of PMPs submitted to the IPC in the period immediately pre, during and post the 2021 Report.

2. Purpose

The PPIP Act requires that all agencies are to have a PMP. Culturally, a PMP needs to be considered as a strategic document that is more than simply a compliance requirement under the PPIP Act. An effective PMP supports the core privacy management principles established under the PPIP Act, but also facilities good privacy practices being built into agency decision-making as well as the design and structure of its systems, business processes, products and service delivery. Importantly, it serves to enable sound privacy governance and practice through both the identification of and understanding of personal and health information holdings throughout the information management lifecycle within agency settings.

This identification and understanding of personal and health information holdings is critical in light of the commencement of the Mandatory Notification of Data Breach (MNDB) Scheme in November 2023. The MNDB Scheme requires agencies to have a plan to include provisions relating to procedures and practices used by the agency to ensure compliance with obligations set out in Part 6A for MNDB Scheme[6]. There is a demonstrable nexus in the understanding and identification of the personal and health information holdings of an agency in its PMP and its ability to sufficiently identify (and respond) when a data breach has occurred.

One of recommendations of the 2021 Report included that there would be a follow-up audit 12 months' time from the 2021 Report. For the purposes of this review, the agencies that were captured as part of the 2021 Report were again reviewed, together with a further additional sample selection of agencies from the local government sector. Additionally, the review also considered the number of PMPs submitted to the IPC subsequent to the 2021 Report as compared to prior years.

[6] Section 33(2)(c1) of the *Privacy and Personal Information Protection Amendment Bill 2022*

3. Findings of the desktop audit

3.1 Limitations

In undertaking this review, no assessment or analysis has been undertaken as to the completeness or comprehensiveness of the PMP. The IPC acknowledges that the review and its analysis reflect a point in time, and that updates may have occurred and are therefore not reflected in the findings or observations made in this report.

3.2 Conduct of the analysis

The analysis of the PMP compliance was undertaken during December 2022. IPC staff examined the PMPs available on sample agency websites, in conjunction with its own data to assess the number of PMPs which had been submitted to the IPC as required by section 33 of the PPIP Act.

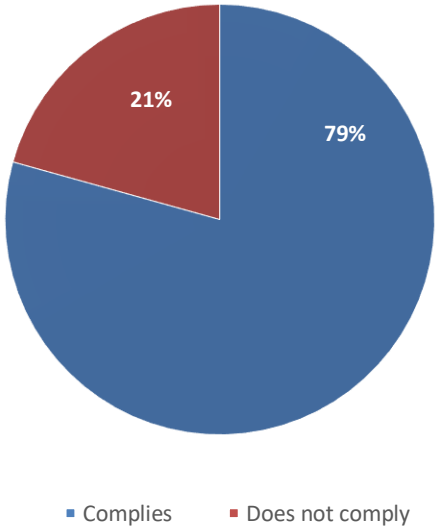
The IPC recorded and retained data in undertaking its review; and for the purposes of this report, it was deemed unnecessary to provide a breakdown for each agency as the findings and recommendations made are applicable generally and not specifically.

3.3 Was a PMP submitted for review in 2022?

3.3.1 Did agencies that were subject of the 2021 Audit Report provide a PMP for review to the IPC in 2022?

Table 1 – provides breakdown of the PMPs that were submitted in 2022 by agencies that were included in the 2021 Report.

Table 1 - Total of agencies that submitted a PMP in 2022



Findings

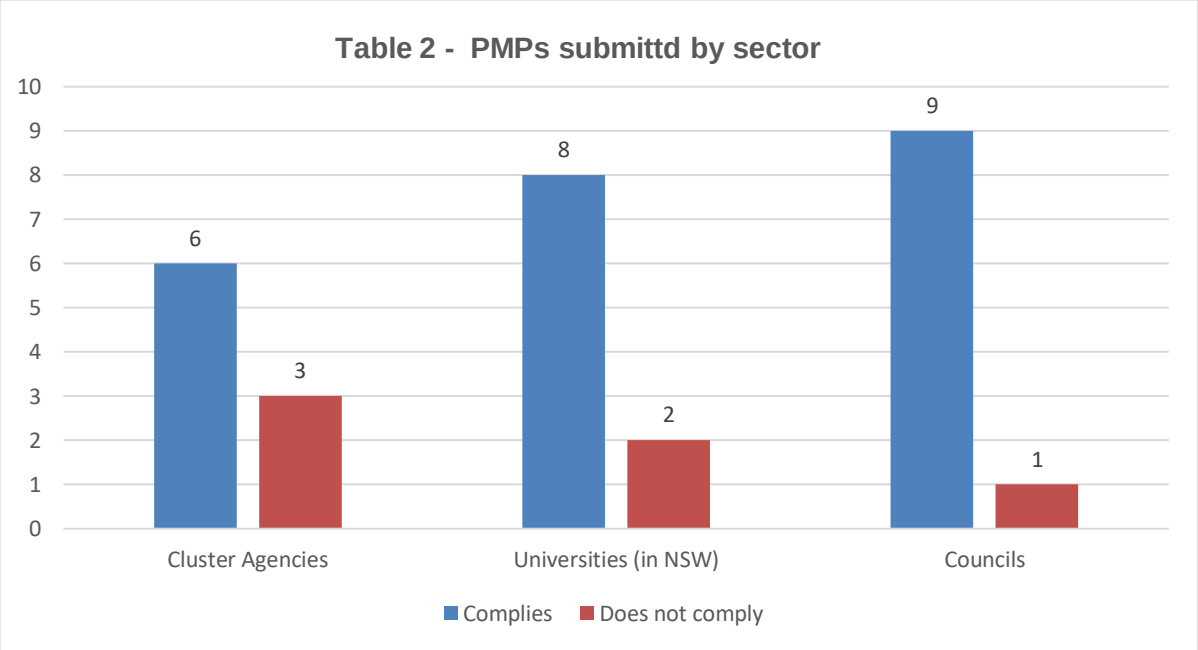
- 73% (23) agencies submitted a PMP for review to the IPC in 2022
- 21% (6) agencies did not submit a PMP for review to the IPC in 2022
- 61% (14) submitted their PMP on or before 30 June 2022. The remaining 39% (9) of agencies submitted their PMP for review after 30 June 2022; with universities representing the timeliest cohort

- The reasons for non-submission of the PMP varied with some advising that they had yet to commence a review of their PMP.

Better practice observations

- Annual review of a PMP contributes to its value and currency. The engagement by the IPC post the 2021 Report contributed to a positive outcome in which the local government sector demonstrated a strong response in submitting PMPs for review in 2022.

Table 2 – provides the breakdown of the PMPs that were submitted in 2022 by agencies that were included in the 2021 Report based on regulated sectors.



Findings

- 79% (23) reviewed in the 2021 Report submitted a PMP to the IPC in 2022
- Of those 79%, 39% (9 agencies) were from the local government sector; 35% (8 from the university sector) and 26% (6 from the public sector)
- 90% (9) of all the local government sector agencies from the 2021 Report submitted a PMP for review in 2022
- 80% (8) of all the University sector agencies from the 2021 Report submitted a PMP for review in 2022
- 67% (6) of all cluster agencies from the 2021 Report submitted their PMP for review in 2022.

Better practice observations

- Inclusion of annual review of a PMP as part of an agency legislative compliance program facilitates an agency's timely review and submission as required by section 33(5) of the PPIP Act.

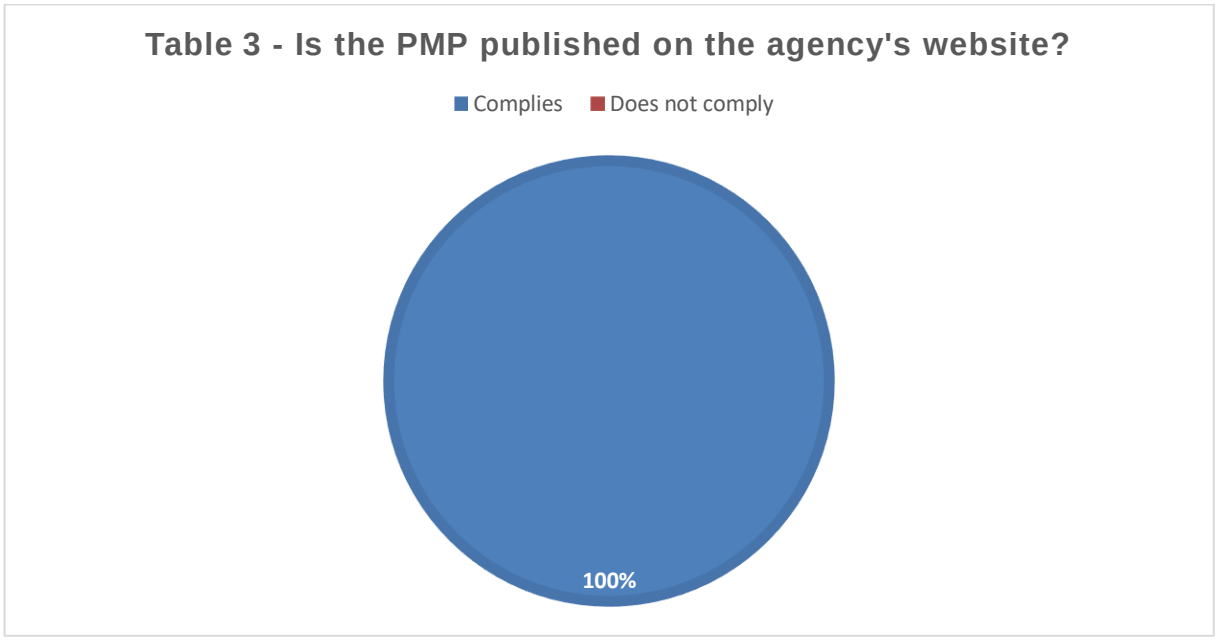
Recommendation 1: It is recommended that those agencies that have yet to commence a review of their PMP take steps to do so as a matter of priority to bring their PMP into currency.

3.4 Existence of PMP – additional agencies

For the purposes of this follow-up review, the IPC extended the scope of those entities it reviewed as part of the desktop review to include a further ten local councils. In undertaking the review, it applied the same key three criteria that were applied in the 2021 Report.

3.4.1 Does the PMP exist on the agency website?

Table 3 – provides the breakdown of whether the additional agencies included to the follow-up review had their PMP published on the agency's website.



Findings

- 100% (10) of the local government sector that were reviewed had pleasingly published their PMP to the agency website
- Although PMPs were published, the ease with which to locate them varied. 70% (7) agencies made their PMPs easily locatable on their website on a dedicated privacy page, whilst the remainder agencies found their PMP to be in various subsites linked to their policies and procedures libraries
- All the PMPs were accessible as standalone pdf files.

Better practice observations

- PMPs were more easily locatable when they were clearly labelled as a Privacy Management Plan and the ease of navigation to locate on the agency website was not overly complex or difficult. This contributed to the searchability of the PMP on the agency website
- PMPs that were labelled as a Privacy Policy were more difficult to identify and distinguish
- PMPs were generally easier to locate when captured and labelled as a PMP as part of the agency 'Privacy' webpage

- PMPs that were accessible on websites in different and non-contradictory forms promoted ease of location. Some agencies adopted a .html website format for the PMP which did not always easily include the most current revision date for the PMP. Agencies should ensure that the most current revision date of their PMP webpage is provided.

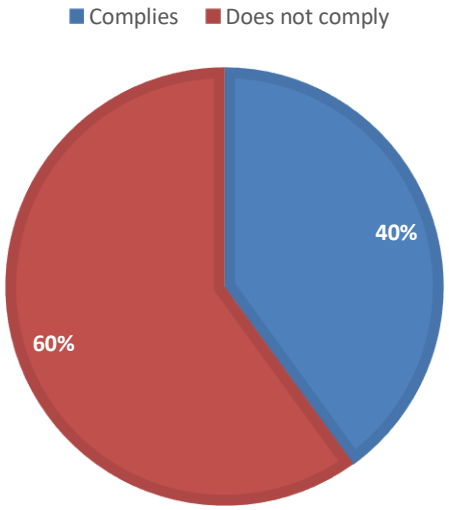
Recommendation 2: It is recommended that agencies review and consider the labelling attached to their privacy management plan to ensure that they are clearly identifiable and distinguishable from other privacy policies.

Recommendation 3: It is recommended that agencies review and consider the presentation of their PMP on agency websites to ensure that the revision date for the PMP is included and clearly apparent.

3.4.2 Currency of the PMP

Table 4 – provides the breakdown of the extent to which the published PMP provided a date of review that fell within the immediate past 12 months from the time of the desktop review.

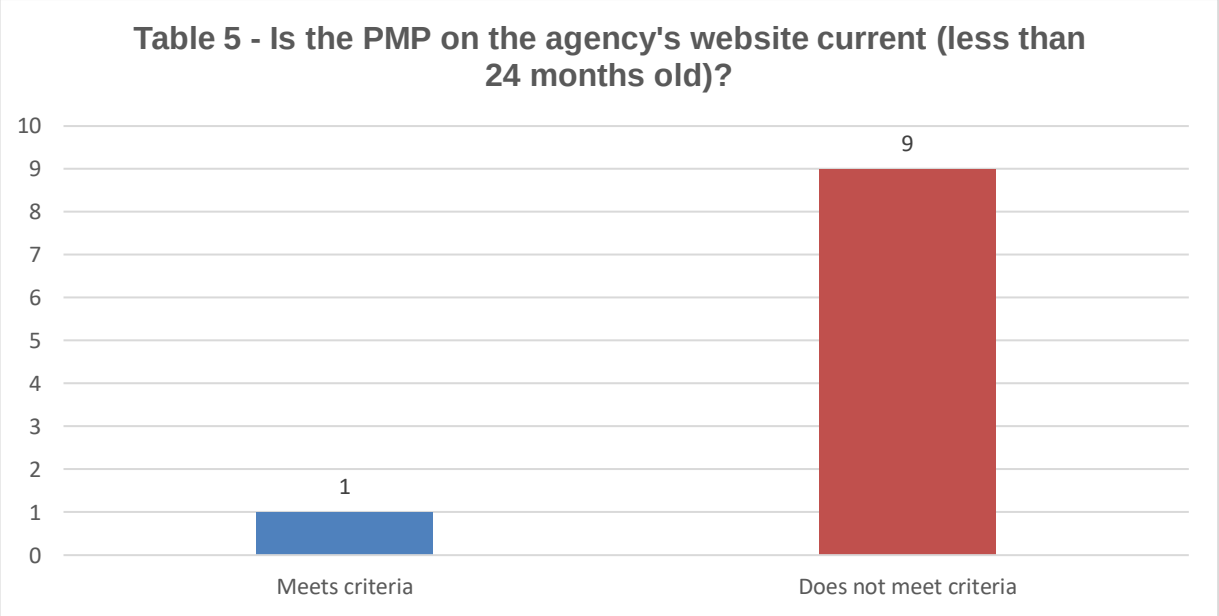
Table 4 - Does the Agency's PMP have a review date of within the immediate past 12 months?



Findings

- The review found that PMPs found on agency websites ranged widely in whether they were current as of the preceding immediate 24 months
- 60% (6) agencies were observed to have a PMP that had a review date of within the immediate past 12 months from when the desktop review was undertaken
- 40% (4) of the agencies had a PMP which provided a review date that was within the immediate past 12 months from when the desktop review was completed.

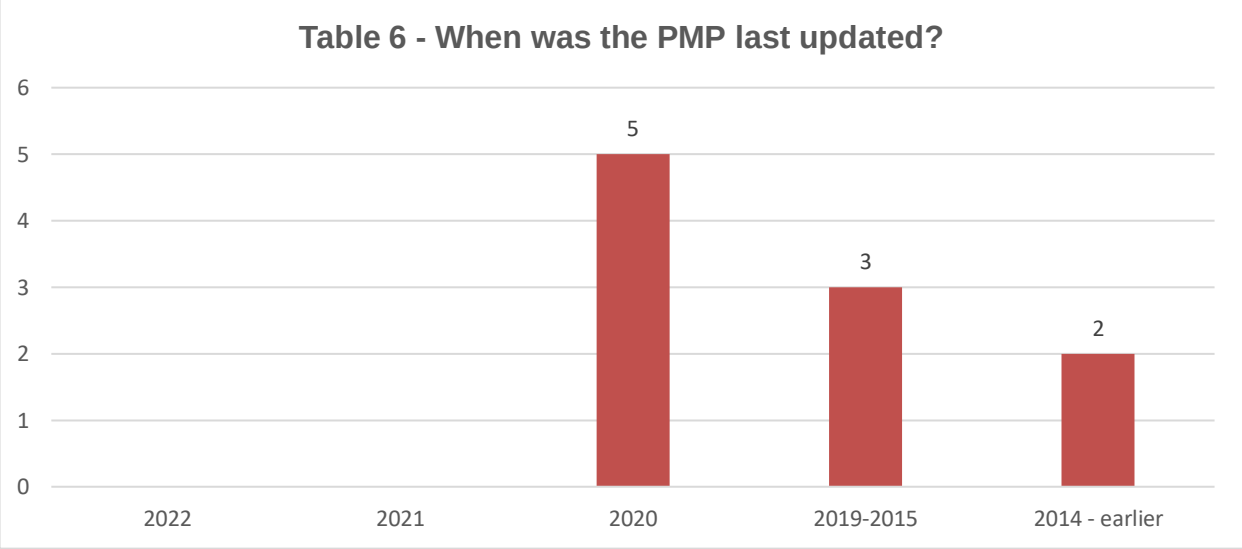
Table 5 – provides the breakdown of the currency of the PMPs, measured by reference to how old the published PMP was and whether, at the point of review, the PMP was less than 24 months old at the time of the review.



Findings

- The review found that PMPs found on agency websites ranged widely in whether they were current as of the preceding immediate 24 months
- 10% (1) had their PMP dated after 1 December 2020
- 90% (9) agencies had a PMP that was dated earlier than 1 December 2020
- Of the 90% with a PMP dated earlier than 1 December 2020, 44% (4) had a PMP dated between December 2019 and December 2020. The balance were found to have a PMP dated current or earlier than December 2019.

Table 6 – provides the breakdown of the distribution of the currency of the PMPs, measured by reference to the year the PMP was published.



Findings

- 90% (9) agencies had a PMP that was dated 1 December 2020 or earlier
- Of the 90% with a PMP dated 1 December 2020 or earlier, 33% (3) included published PMPs last updated in between the period 2019 – 2015
- 22% (2) were found to have a PMP from earlier than 2014 with at least one dating back to 2010
- The 2021 Report also observed that some PMPs were notably dated, and this review has again found similarly, in a context where it is difficult to rationalise that the personal/health information practices within agencies would be unchanged in a period that would span more than 10 years
- Despite commitments in their respective PMPs to undertake a review at a set and dedicated review date, some PMPs had not been reviewed in a decade.

Better practice observations

- Although, the requirements of section 33 provides that a PMP may be amended at any time and does not stipulate a minimum period for regular review, regular review of PMPs contributed to the minimisation of risks associated with outdated practices and processes relevant to the handling of personal information
- Regular review ensures that policies and practices reflect contemporary application and interpretation of case law to the collection, handling and management of personal/health information over the information management cycle
- The Privacy Commissioner's recommendations contained in the 2021 Report stressed the importance of conducting regular and frequent reviews of their PMPs at a period of every 12 months
- The increasing adoption of digital platforms, both as a tool to facilitate agency functions and for service delivery are best supported by frameworks, policies and practices which are regularly reviewed and reflect the applicable arrangements within operating environments
- Agencies that regularly review their PMPs for currency are better placed to implement the requirements of the MNDB Scheme to provide for the procedures and practices to be used by the agency to ensure its compliance with the obligations and responsibilities for the MNDB Scheme. This is because the agency's identification and understanding of its personal information/health information as provided for in its PMP will be reflective of current practices and arrangements from which its procedures or the MNDB Scheme will be informed.

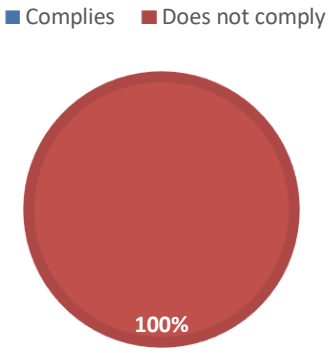
Recommendation 4: It is recommended that any agency that has not reviewed their PMP in the last 12 months do so as a matter of priority. In doing so they should also have regard to the requirements of the upcoming MNDB Scheme in the revision of their PMP.

Recommendation 5: It is recommended that agencies implement regular review of their PMP at least every 12 months. The review of the PMP be included as part of the agency's framework for legislative/policy review registers and included as part of its compliance reporting to Audit and Risk Committees or equivalent.

3.4.3 Legislative compliance - number of PMPs submitted to the IPC

Table 7 – provides the breakdown of the legislative compliance with the requirements of section 33(5) of the PPIP Act by the additional agencies included in the review in providing a copy of their PMP in instances where their PMP had indicated a review that took place in the past 12 months.

Table 7 - Do the IPC's records demonstrate that the agency submitted a PMP for review in the immediate past 12 months?



Findings

- No agencies complied with section 33(5) of the PPIP Act in providing the Privacy Commissioner with a copy of their PMP in instances where their PMP had indicated a review that took place in the past 12 months.

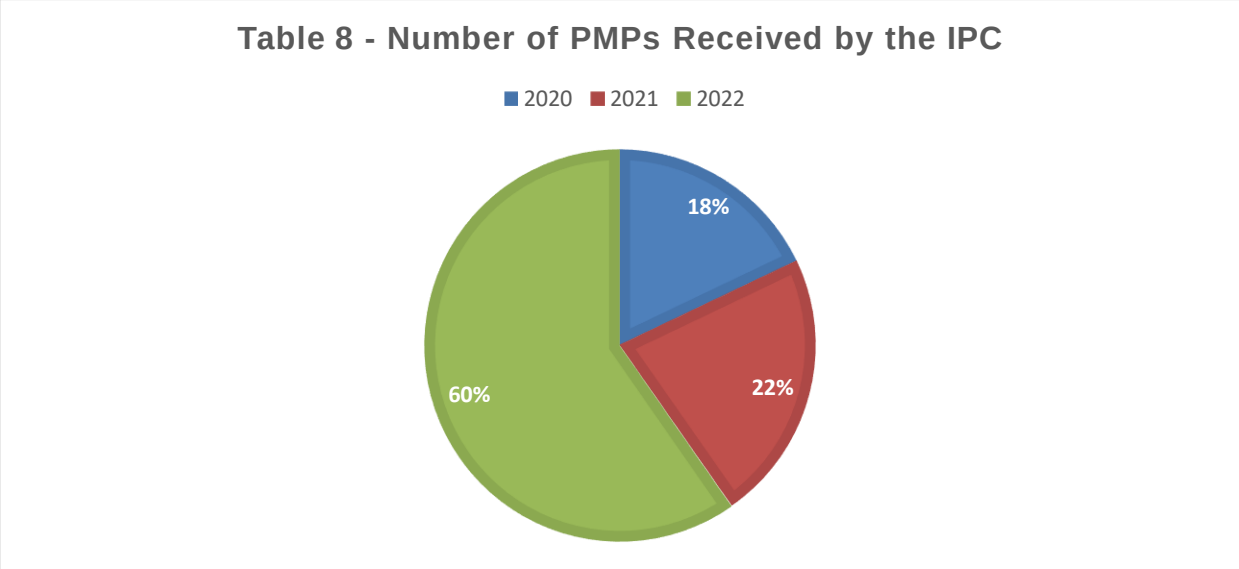
Better practice observations

- Establishing processes for PMP review that included the submission to the Privacy Commissioner ensured that the compliance requirements as provided by section 33 (5) of the PPIP Act were satisfied.

Recommendation 6: It is recommended that agencies have an established and documented process for PMP review which includes the requirements necessary to achieve compliance with section 33(5) of the PPIP Act.

3.5 Level of submission of PMPs to the IPC period immediately pre, during and post the 2021 Report.

Table 8 – provides the numerical distribution of the legislative compliance with the requirements of section 33(5) of the PPIP Act in providing a copy of their PMP immediately pre, during and post the 2021 Report.



Findings

- Across the 3 calendar years a total of 67 agencies had provided their PMP to the Privacy Commissioner in accordance with section 33(5) of the PPIP Act
- 60% (40) of agencies provided their PMPs in 2022, the highest number of the 3 calendar years. This includes 23 of the agencies that had been included in the 2021 Report
- 22% (15) of agencies submitted a PMP to the IPC for review in 2021. 18% (12) of agencies submitted a PMP to the IPC for review in 2020
- The number of PMPs increased post the 2021 Report and demonstrated the value in the desktop compliance activity undertaken and the subsequent proactive engagement taken by the IPC following the publication of the 2021 Report.

Better practice observations

- Establishing processes for PMP review that included the submission to the Privacy Commissioner ensured that the compliance requirements as provided by section 33 (5) of the PPIP Act were satisfied.

4. Conclusions

The findings in the follow-up review identify that progress has occurred in relation to those agencies that were captured within the initial audit scope in which a significant number reviewed their PMPs as a result. This was further reflected in the notable increase in the number of PMPs that were submitted to the IPC in 2022 as compared to previous years. The positive change which reflects an appreciation of the importance and role of a PMP is welcome.

However, this follow-up audit has again identified that currency and review of PMPs continues to remain an issue. The 2021 Report included recommendations to promote better practices for PMPs and despite this, this follow-up audit has made further recommendations which in some ways are similar in nature to those made in the 2021 Report. The inclusion of the additional agencies to the scope of the follow-up audit has identified that it continues to remain the case that although PMPs are accessible and locatable on agency websites, the currency, age and frequency of review of those PMPs remains an area which requires attention. There is little value in agencies publishing PMPs which are out of date and do not reflect current practices or arrangements

These results of the additional agencies tend to indicate an absence of consideration of the purpose and role of PMPs for both staff, and the citizen more generally. This is the second consecutive report which has highlighted the concerns around the currency of PMPs. It continues to highlight a lack of inclusion of PMPs as part of the broader governance arrangements, with clear opportunity for improvements to be made, with a focus to those specific agencies, and across all regulated entities subject to the PPIP Act that may ultimately require legislative amendments to bring the compliance requirements for a PMP in line with similar requirements for agencies that are required to have an Agency Information Guide (AIG) under the *Government Information (Public Access) Act 2009.* Those requirements provide a legislative mechanism to require agencies to review its AIG and adopt a new AIG at intervals of not more than 12 months.

In the absence of legislative requirements, it falls to the agency leadership to take the steps needed to achieve and maintain PMPs which have currency and provide value.

Agency leaders are strongly encouraged to consider and implement the recommendations of this report in order to elevate compliance in relation to the handling of personal information, assist in preparing for the introduction of the MNDB Scheme and support the delivery of digital services to the public.

5. Recommendations

Based on the findings from this follow-up review, agencies should take prompt action to implement measures informed by the findings of this desktop review. By doing so, agencies will not only meet their compliance requirements under section 33(5) of the PPIP Act, but will also better reflect robust privacy governance.

Arising from the findings in this review, it is recommended that agencies review and implement where required the following recommendations. These recommendations should be considered in conjunction with those made in the 2021 Report.

Recommendations	
Recommendation 1:	It is recommended that those agencies that have yet to commence a review of their PMP take steps to do so as a matter of priority to bring their PMP into currency.
Recommendation 2:	It is recommended that agencies review and consider the labelling attached to their privacy management plan to ensure that they are clearly identifiable and distinguishable from other privacy policies.
Recommendation 3:	It is recommended that agencies review and consider the presentation of their PMP on agency websites to ensure that the revision date for the PMP is included and clearly apparent.

Recommendation 4:	It is recommended that any agency that has not reviewed their PMP in the last 12 months do so as a matter of priority. In doing so they should also have regard to the requirements of the upcoming MNDB Scheme in the revision of the PMP.
Recommendation 5:	It is recommended that agencies implement regular review of their PMP at least every 12 months. The review of the PMP be included as part of the agency's framework for legislative/policy review registers and included as part of its compliance reporting to Audit and Risk Committees or equivalent.
Recommendation 7:	It is recommended that agencies have an established and documented process for PMP review which includes the requirements necessary to achieve compliance with section 33(5) of the PPIP Act.

6. Monitoring

The IPC will continue to assist agencies to adopt these recommendations and provide regulatory assistance to improve their compliance.

Appendix A: Audit Methodology

The review was undertaken with reference to the Privacy Commissioner's functions under section 36 of the PPIP Act.

The review was limited to:

- A desktop assessment and review of the agency compliance with having a PMP under section 33;
- A review of agency websites; and
- IPC data based on the number of PMPs notified to the IPC by agencies.

As a regulatory tool, a desktop approach is applied in areas of small to moderate risk of noncompliance and may also form the basis of a preliminary assessment. The methodology should be recognised as constrained by factors, including:

- independent remote assessment;
- non inquisitorial; and
- focused on identifying compliance risks.

On that basis, it is distinguishable from an onsite review which can adopt a more inquisitorial approach. Accordingly, the IPC conducts desktop reviews to elevate compliance by way of guidance, awareness raising, and as required make recommendations to a department.

Limitations

In undertaking this review, no assessment or analysis has been undertaken as to the completeness or comprehensiveness of the privacy management plan. The IPC acknowledges that the review and its analysis reflect a point in time, and that updates may have occurred and are therefore not reflected in the findings or observations made in this report.

Conduct of the analysis

The analysis of the PMP compliance was undertaken over December 2022. IPC staff examined the PMPs available on sample agency websites, in conjunction with its own data to assess the number of PMPs which had been submitted to the IPC as required by section 33 of the PPIP Act.

The IPC recorded and retained data in undertaking its review; and for the purposes of this report, it was deemed unnecessary to provide a breakdown for each agency as the findings and recommendations made are applicable generally and not specifically.

2021 Report Agencies

Consists of those agencies that were audited as part of the 2021 Report and include:

1. Nine NSW Government agencies;
2. Ten Universities within NSW; and
3. Ten local government councils.

A desktop review of these agencies was completed against the following audit criteria:

1. Whether the IPC's records show that the 2021 Report agencies submitted a PMP for review in the 2022 calendar year following the 2021 Report.

Follow-up report additional sample agencies

Consists of ten randomly selected local government councils from across NSW, reflecting an even distribution between urban and rural areas as follows:

1. Five urban local government councils; and
2. Five rural local government councils.

A desktop review of each against the following three audit criteria items was completed:

1. Existence of a PMP on an agency website;
2. The currency of the PMP, including whether the PMP has a review date of within the immediate past 12 months; and
3. Where a PMP exists on an agency website and identifies as having been reviewed within the immediate past 12 months, whether the IPC's records demonstrate whether that PMP was submitted for review to the IPC.

PMP notification to the IPC

Consists of a desktop review of the number of PMP's submitted to the IPC in 2020, 2021 and 2022.

Scope

In respect of 2021 Report agencies, the scope is limited to capturing the extent to which agencies submitted a PMP for IPC review in 2022 in response to the report, recommendations and engagement by the IPC.

In respect of follow-up report additional sample agencies, the scope of the desktop audit is limited to a verification of the existence of a PMP and is thus a benchmark exercise.

In respect of PMP notification to the IPC, the scope of the desktop audit is limited to a numerical review of the number of PMP's received by the IPC from agencies in the calendar years 2020, 2021 and 2022; for the purposes of assessing whether the number of PMPs is stable or increasing.

In respect of all agencies, the assessment of the content of the PMP and any review against the PMP check list is out of scope.

Appendix B: Audit chronology

Date	Event
16 December 2022	Desktop Audit assessment completed
January – June 2023	Analysis and Report Drafting
30 June 2023	Final Report Published

Appendix C: Abbreviations

The following table lists the commonly used abbreviations within this report.

Acronym or abbreviation	Explanation
AIG	Agency Information Guide
PMP	Privacy Management Plan
PPIP Act	*Privacy & Personal Information Protection Act 1998* (NSW)
HRIP Act	*Health Records & Information Privacy Act 2002* (NSW)
2021 Report	The Desktop Audit Privacy Management Plans (PMP) Report published by the Privacy Commissioner in December 2021
PPIP Bill	*Privacy and Personal Information Protection Amendment Bill 2022* (NSW)
MNDB Scheme	Mandatory Notification of Data Breach Scheme

Appendix D: Legislation

Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)

Division 2 - Privacy management plans

33 Preparation and implementation of privacy management plans

(1) Each public sector agency must prepare and implement a privacy management plan within 12 months of the commencement of this section.

(2) The privacy management plan of a public sector agency must include provisions relating to the following -

> *(a) the devising of policies and practices to ensure compliance by the agency with the requirements of this Act or the Health Records and Information Privacy Act 2002, if applicable,*
>
> *(b) the dissemination of those policies and practices to persons within the agency,*
>
> *(c) the procedures that the agency proposes to provide in relation to internal review under Part 5,*
>
> *(d) such other matters as are considered relevant by the agency in relation to privacy and the protection of personal information held by the agency.*

(3) (Repealed)

(4) An agency may amend its privacy management plan from time to time.

(5) An agency must provide a copy of its privacy management plan to the Privacy Commissioner as soon as practicable after it is prepared and whenever the plan is amended.

(6) The regulations may make provision for or with respect to privacy management plans, including exempting certain public sector agencies (or classes of agencies) from the requirements of this section.

36(2) General Functions

In particular, the Privacy Commissioner has the following functions –

To provide assistance to public sector agencies in preparing and implementing privacy management plans in accordance with section 33.