information and privacy commission
new south wales

Desktop Audit of Privacy Management Plans (PMP) Report

December 2021

Contents

Executive Summary

A Privacy Management Plan (**PMP**) is a strategic planning document in which each public sector agency describes the measures it proposes to take to ensure that it complies with the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) and the *Health Records and Information Privacy Act 2002* (**HRIP Act**).

NSW public sector agencies as required by section 33 of the PPIP Act, must have a PMP. It should also be made publicly available on the agency's website and made available in other ways on request. Section 33 of the PPIP Act further provides that agencies must provide a copy of their PMP to the Privacy Commissioner as soon as practicable after preparation or amendment.

On 18 December 2020, the NSW Audit Office released its special report *Service NSW's handling of personal information* which included observations as to the currency of Service NSW's PMP.[1] During evidence to the NSW Parliament Cybersecurity Inquiry the Privacy Commissioner, in noting the resource limitations of the Information and Privacy Commission **(IPC**), observed that the IPC would be following up agencies about the currency of privacy management plans.[2] The Privacy Commissioner subsequently published in July 2021 her intention to undertake a review of the existence and currency of privacy management plans by way of a desktop review.[3] That desktop review was foreshadowed for Q2 of 2021/22.

In November 2021, **IPC** commenced a desktop review to assess the following agencies that fall under the jurisdiction of the PPIP Act including:

1. NSW Government agency cluster departments;
2. Universities within NSW; and
3. Ten selected local government councils identified through the intelligence holdings of the IPC[4] that have either had a breach found in an internal review or had an instance of review that was high.

A desktop review of each agency's PMP against the following three audit criteria items was completed:

1. Existence of a PMP on an agency website;
2. Currency of PMP, including whether the PMP has a review date of within the immediate past 12 months, i.e. from November 2020 to November 2021; and
3. If a PMP exists on an agency website, whether the IPC's records demonstrate whether that PMP was submitted.

This review did not include an assessment as to the accuracy or completeness of the PMP itself as this was out of scope for the purposes of this review.

---

[1] *Audit Office Special Report on Service NSW's handling of personal information at p4.*

[2] *NSW Parliament, Cybersecurity report at p27.*

[3] *Information and Privacy Commission at https://www.ipc.nsw.gov.au/ipc-privacy-proactive-regulatory-initiatives-program-202122*

[4] *Intelligence report dated (Month), 2021 into breaches found in agency internal reviews or high instances of internal reviews undertaken by regulated agencies. Ten councils that were either found to have a breach or a high instance of internal reviews as a result of the findings of the intelligence report were selected by the IPC's Compliance Committee.*

In relation to the three audit criteria items, the IPC found that:

1. All agencies were compliant to the extent that a PMP is published and exists on their respective website;
2. Most agencies have made their PMPs easy to locate; whilst others required far more substantive searching to locate their PMP;
3. The currency of PMPs found on agency websites ranged widely in whether they were current within the preceding immediate 12 months, with only 6 out of 29 audited agencies having a currency date in that time period;
4. Only 6 out of 29 audited agencies had a review date of within the immediate past 12 months, including four cluster departments and two universities. No councils were found to be compliant against this criterion;
5. Of the 6 agencies that had a review date of within the immediate past 12 months, 3 agencies submitted their PMP to the IPC for review, consisting of two cluster departments and one university;
6. Agencies could generally improve their PMP reviewing practices by ensuring that the frequency of review is undertaken in a shorter timeframe; and
7. Agencies could improve in ensuring that their PMPs are accessible in-full and in readable file formats such as pdf.

1. Background Methodology

1.1. Role of the Privacy Commissioner

The role of the Privacy Commissioner under the PPIP Act includes:

- Providing assistance to public sector agencies in adopting and complying with the information protection and health protection principles and privacy codes of practice;
- Initiating and recommending the making of privacy codes of practice; and
- Providing advice on matters relating to the protection of personal information and health information and the privacy of individuals.

In accordance with Section 33 of the PPIP Act, agencies must prepare and implement PMPs. Agencies must also provide a copy of their PMPs to the Privacy Commissioner as soon as practicable after they are either prepared or amended.

To assist agencies, the IPC has published privacy resources and guidance that are specifically tailored for the formulation of NSW public sector agency PMPs. These resources extend to guide agencies on how to make a PMP as well as a PMP Assessment Checklist which aids as a tool to help agencies assess existing or preparing PMPs.

The Privacy Commissioner's guidance relevantly recommends that:

- Public sector agency PMPs are made publicly available to ensure that members of the public understand; how to make a complaint or request an internal review, how to access their personal or health information, how the agency is accountable for its management of personal or health information;

- Public sector agencies review their PMPs at regular intervals, such as every 12 months, or preferably no more than every two years;
- Public sector agencies set a review date and clearly communicate that review date in their PMP; and
- Public sector agencies should review and update their PMP when the agency's functions, structure, activities or technological systems change the way in which they manage personal or health information.

This guidance also states that PMPs should be made publicly available on the agency's website and made available in other ways on request.

1.2. Importance of privacy management plans

PMP plans are an important element and input of an agency's governance. They serve an important role in explaining how an agency manages personal and health information under NSW privacy laws. PMPs provide information about the personal information an agency collects and retains, how to access and amend personal information and the actions an individual may take under privacy laws.

As a strategic planning document, the PMP describes the measures it takes to ensure that it complies with the PPIP Act and HRIP Act.

PMPs are important to the extent that they allow agencies to transparently demonstrate to members of the public:

- How the requirements of the PPIP Act and HRIP Act apply to the personal information and health information it manages;
- The functions and activities and the main types of personal information or health information they deal with to carry out their functions and activities;
- Any relevant exemptions that an agency may commonly rely upon under the PPIP Act;
- The strategies they employ to comply with the PPIP Act and HRIP Act;
- That staff are provided with the necessary knowledge and skills to manage personal information and health information appropriately;
- How to make a complaint or request an internal review in the event they consider that their privacy has been breached;
- How to request access to their personal information or health information or an amendment to that information to ensure its accuracy; and
- That they are accountable for their management of personal information and health information.

Ensuring the currency of an agency's PMP is central to fulfilling its purpose, particularly in an environment of increasing digital transformation in the way that agencies undertake their functions and deliver services.

1.3. Purpose

The purpose of this desktop review is to gain a baseline measure of the existence and currency of PMPs publicised on agency websites and the extent to which those same documents have been provided to the IPC in accordance with the Privacy Commissioner's functions under Section 33(5) of the PPIP Act.

1.4. Scope

The scope of the desktop audit is limited to a verification of the existence of a PMP and is thus a benchmark exercise.

The assessment of the content of the PMP and any review against the PMP check list is out of scope.

The public sector agencies that fall in scope under the desktop audit are:

1. NSW Government agency cluster departments;
2. Universities within NSW; and
3. Ten selected local government councils through the intelligence holdings of the IPC that have either had a breach found in an internal review or had an instance of review that was high.

1.5. Methodology

The desktop analysis considered whether:

1. A PMP existed on the agency's website;
2. Currency of the PMP including whether it had a review date of within the immediate past 12 months; and
3. Whether IPC records showed that the PMP was submitted.

The agency PMPs were downloaded from their respective websites in November 2021 and these documents formed the basis of the following analysis.

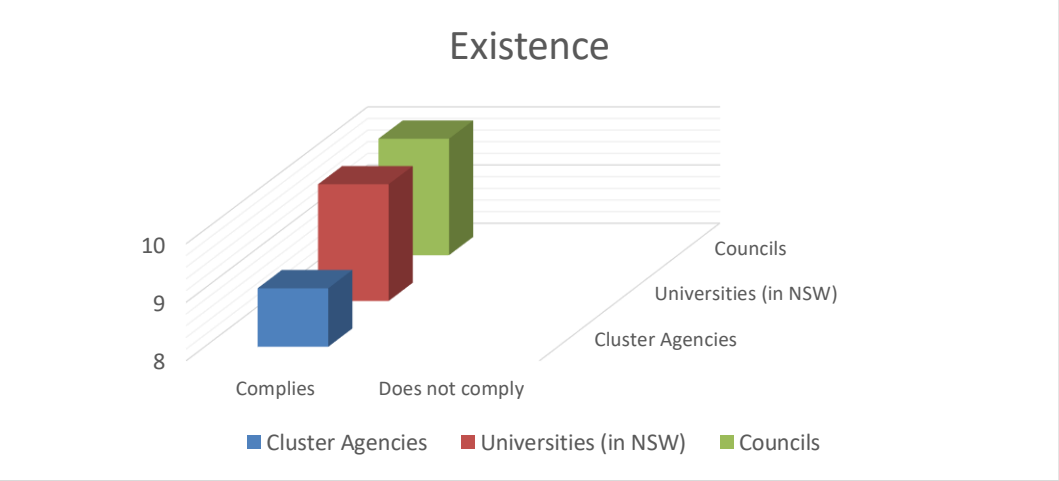
The desktop analysis reflects a point in time, and the IPC acknowledges that it may be the case that updates may have occurred subsequent to the analysis and are therefore not reflected in the following findings or observations.

2. Findings in respect of desktop audit criteria

2.1. Does the PMP exist on the agency website?

As part of conducting the desktop audit review against this criterion, the IPC reviewed the dedicated websites of each of the public sector agencies that were in scope.

All public sector agencies that fell in scope of the review were found to be compliant in respect of the fact that a PMP does exist on their website.



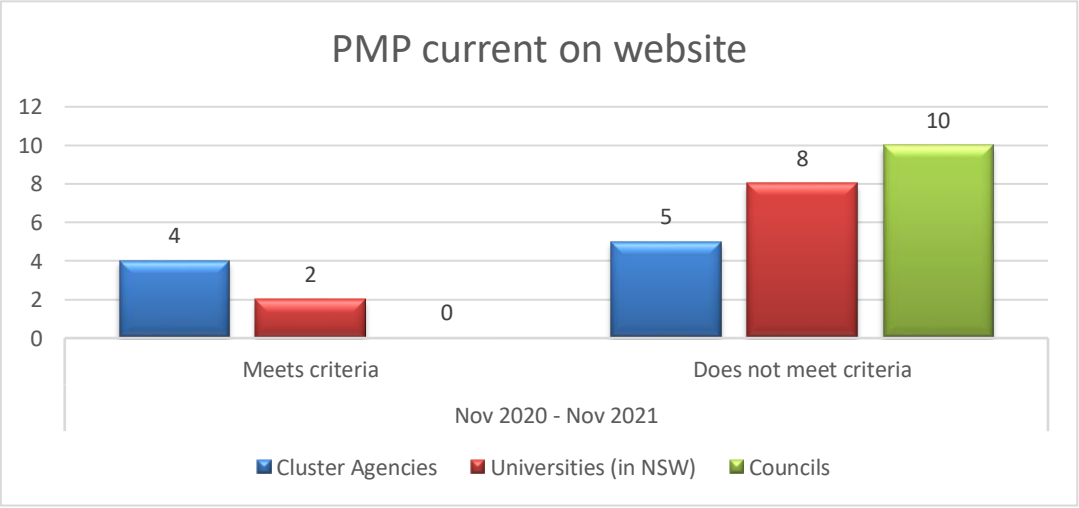
There were variations in difficulty in locating the privacy management plans on agency websites. Some PMPs were located in their dedicated privacy pages, others in their access to information pages and others in their policies and procedures page.

Additionally, the form which PMPs took also varied between public sector agencies, with a majority of PMPs being accessible as standalone pdf files, others located in an agency privacy policy and others in a website html format. The value and benefit of a PMP can be constrained if its accessibility and ease of location is overly complex and difficult to locate.

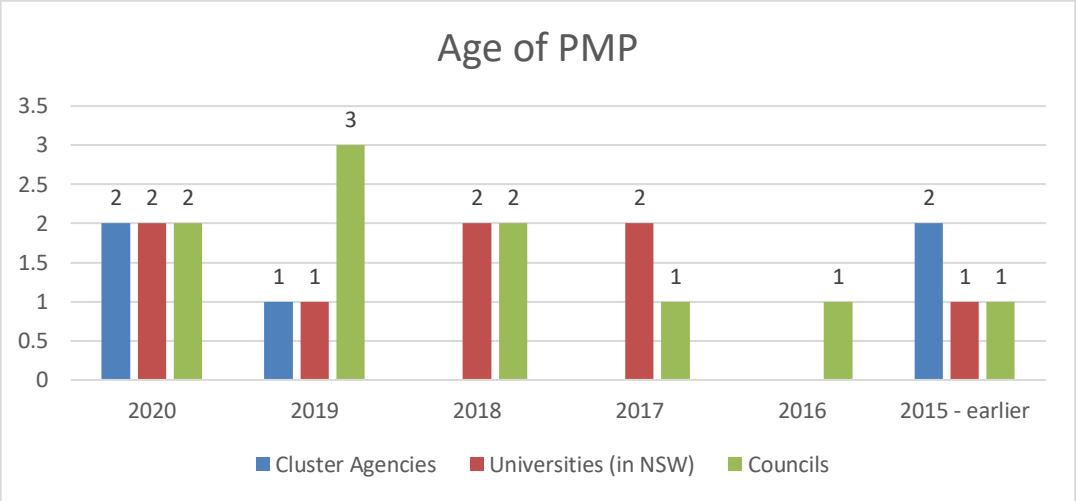
2.2. Are the PMPs current?

Having established that PMPs existed on agency websites, this review then considered the currency of the PMPs that were located on the agency website measured by reference to how old the published PMP was and whether the PMP was more than 12 months old. (at the point of review)

The review found that PMPs found on agency websites ranged widely in whether they were current as of the preceding immediate 12 months. Of the 29 agencies in scope, 6 agencies, consisting of 4 cluster departments and 2 universities were identified as being dated or current as between November 2020 and November 2021. No local government council PMPs were found to have been dated or current in that time period.



Of the 23 agencies that did not have a PMP in the period 2020-2021, 19 had a PMP dated within the period November 2015 to November 2020. This was represented as 3 cluster departments, 7 universities and 9 local government councils. The balance of 4 agencies consisting of, 2 cluster departments, 1 university and 1 local government council were found to have their PMPs dated or current earlier that November 2015. This means that of all 29 agencies reviewed, 17 agencies' PMPs (59%) were dated 2 years or more since published.



Although, the requirements of section 33 provide that a PMP may be amended at any time and do not stipulate a minimum period for regular review, in a context of machinery of government changes and the increasing adoption of digital platforms both as a tool to facilitate agency functions and for service delivery, it would be reasonable to conclude that this would necessitate a review of the PMP and some consideration at least of what this may mean for personal information and or health information under a PMP. It is difficult to imagine that this would not lead to some kind of amendments, even if only minor.

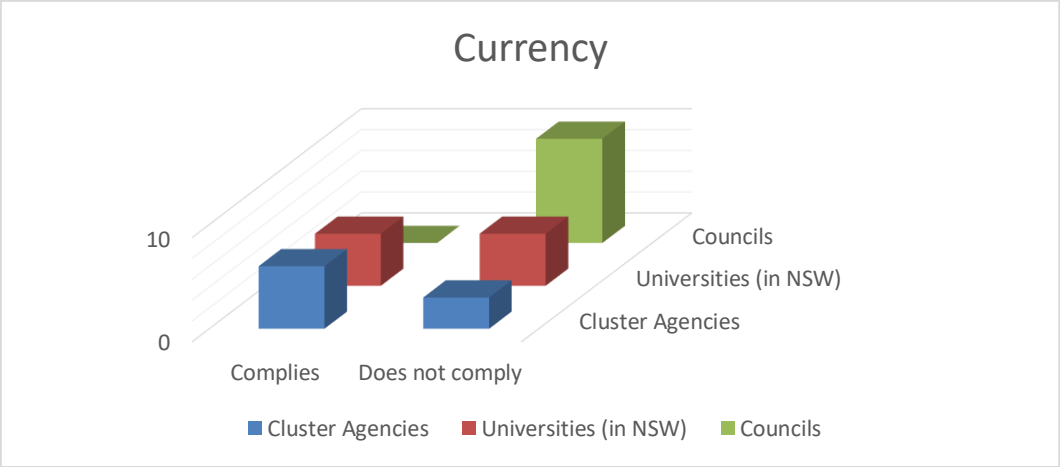
2.3. Does the PMP itself have a review date of within the immediate past 12 months?

Following consideration of the currency of the PMP, the desktop review focused on whether the PMPs found on the agency websites provided a review date within the immediate past 12 months in the PMP itself.

In our review we observed that some public sector agencies have not reviewed their PMPs in nearly 10 years; despite commitments in their respective PMPs to undertake a review at a set and dedicated review date.

Despite the guidance provided by the Privacy Commissioner, we also observed that some public sector agency PMPs do not state or provide either a precise review date or an approximate review period in respect of the review of the current iteration of their PMP.

The IPC found that 11 agencies out of a total of 29 complied with this line of enquiry, split between 6 cluster departments and 5 universities. No local government councils were found to have had a review within the immediate past 12 months.



For completeness, the desktop review identified 8 agencies out of 29, consisting of 1 cluster department, 3 universities and 4 local government councils, whose review period was identified to commence after the immediate past 12 months i.e. November 2021 onwards.

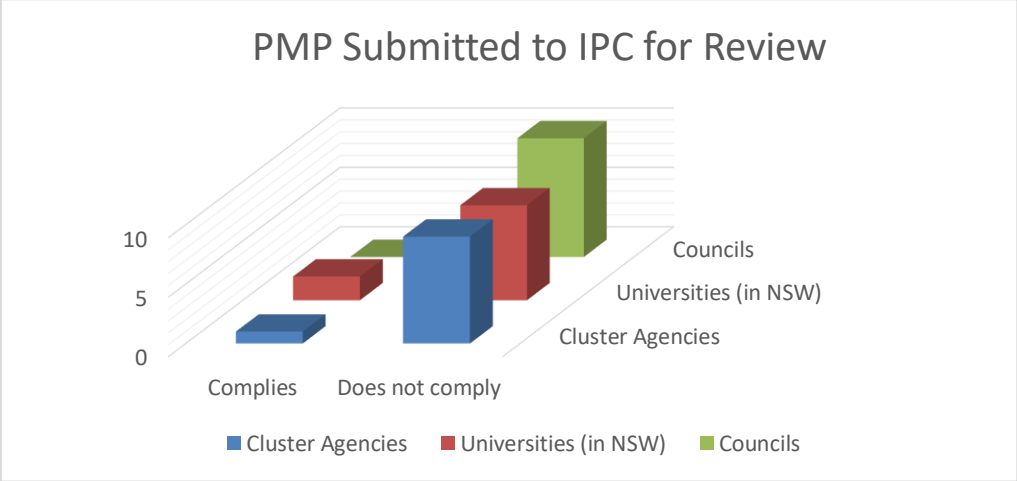
This means that 10 agencies out of 29 in total, consisting of 2 cluster departments, 2 universities and 6 local government councils either had a review date listed before the immediate past 12 months i.e. prior to November 2020 or didn't have a review date listed at all. This result is of concern particularly in circumstances where this review observed PMPs which appeared to be dated more than 3 years ago.

2.4. Do the IPC's records show that the PMP was submitted for review?

Lastly, the IPC examined whether its records demonstrated that they received agency PMPs that were updated and reviewed within the past 12 months for their regulatory review.

The results of the desktop audit review show that 64% of agencies did not comply with section 33(5) of the PPIP Act as a result of not providing the Privacy Commissioner with a copy of their PMP in instances where their PMP had undergone review in the past 12 months.

Out of the 11 agencies that complied with the previous criterion, the desktop audit review found that 1 cluster department and 2 universities had submitted their PMPs to the IPC for their review as at the date of the desktop review.



In respect of those agencies that didn't satisfy the 2nd criterion, 3 cluster departments, 5 universities and 3 local government councils submitted their PMPs to the IPC for review.

In respect of those agencies that didn't satisfy the 2nd criterion, 4 cluster departments, 3 universities and 7 local government councils did not submit their PMPs to the IPC for review.

2.5. Overall Conclusions

In general, agencies are appropriately providing their PMPs as publicly available documents on their dedicated websites. While this would appear a positive result, it needs to be relevantly considered with respect to the currency of the PMP that is available. There is little value in agencies publishing PMPs which are out of date and do not reflect current practices or arrangements.

This review also observed PMPs which are either dated or have a review date in the period between November 2020 and November 2021. Overall, almost a third of PMPs fell into this category. It further observed that only 36% of PMPs dated or having a review date in the immediate 12-month period having been submitted to the IPC for their review. This suggests that either the PMPs have not been reviewed and amended or they were not provided to the Privacy Commissioner or both.

The results of this review tend to indicate an absence of consideration of the purpose and role of PMPs for both staff and the citizen more generally. In particular, it highlights the lack of inclusion of PMPs as part of the broader governance arrangements of regulated entities and that there is opportunity for improvements to be made.

3. Recommendations

PMPs can harbour enormous value and significance when they:

- Demonstrate currency in respect of being relevant and up to date about the programs, services and functions and governance arrangements that a public sector agency has in place;
- Are reviewed regularly, in accordance with the Privacy Commissioner's guidance on PMPs; and
- Are amended and provided to the Privacy Commissioner in accordance with public sector agency obligations under section 33(5) of the PPIP Act.

The recommendations that follow in this report are directed to assisting and supporting all regulated entities to achieve and elevate their compliance with the requirements for privacy management plans. They are informed by the findings and observations arising from the desktop review and present an opportunity for all entities to respond positively by:

1. Reviewing in accordance with s33(5) of the PPIP Act, their legislative compliance under this provision. Where there has been a period of 12 months or more since the agency PMP has been reviewed and amended, agencies should act promptly to review their PMP and in any case no later than within 3 months of this report.
2. Prominently including in all PMPs the date of the PMP and its next review.

3. Developing and implementing a process for regular review and update of the PMP at least every twelve months. That process should be documented and included as part of the agency's governance processes and include a mechanism that enables the provision of an amended PMP to the Privacy Commissioner in a timely manner.
4. Promoting consistency and accessibility in relation to PMPs by establishing a single readily identifiable access pathway that is easily and prominently located on its website and capable of being located from a single search from the main page. This should include meaningful labelling of the PMP with relevant links.
5. Include the review of the PMP as part of its legislative compliance policy/ register.

In addition, the Privacy Commissioner commits to:

1. Engaging with those agencies identified during the review as holding PMPs that lack currency or have not provided their current PMP to the IPC and ensuring that, where appropriate, remediation is taken and tailored towards the reviewing and updating of that agency's PMP as soon as practicable.
2. Revisiting the desktop audit findings, as part of conducting a further audit of agencies PMPs in 12 months-time from the date of this report.

Appendix A: 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.