Agency Privacy Maturity Assessment Survey

Instructions

Agencies should perform the privacy assessment for each area of practice using this survey, which can be completed by privacy officers or released for wider participation.

This survey can be kept together or broken down by area of practice and can be uploaded to Microsoft Forms using the Quick Import function, or to other survey tools for easy collection of responses and viewing of response data.

**Follow the links below to each area of practice:**

[Section 1: Culture and Leadership](#Section_1)

[Section 2: Privacy Reporting](#Section_2)

[Section 3: Data Breach Reporting](#Section_3)

[Section 4: Information Holdings](#Section_4)

[Section 5: Privacy Impact Assessments](#Section_5)

[Section 6: Privacy Functions](#Section_6)

[Section 7: Privacy Management Plans](#Section_7)

[Section 8: Internal Reviews](#Section_8)

The target audience for the surveys is to be determined by officers. Some areas of practice may require widespread distribution to get accurate responses while other may only need to be sent to a set of specific individuals. In smaller agencies, the surveys may only need to be completed by the privacy officer themselves.

To ensure the best use of this survey and its interaction with the Management Document, privacy officers should be encouraged to complete the survey to the best of their understanding.

Surveys and assessment are advised to be completed regularly in order to track maturity levels over time.

*You may wish to delete the above instructions before issuing the survey*

About this Survey

This survey is a tool to support privacy officers in understanding the nature and effectiveness of their Agency’s privacy practices.

Please respond to this questionnaire to the best of your understanding and judgement.

Confident and accurate assessments of the Agency’s current maturity status will allow for an understanding of areas for improvement, and planning of targeted improvement activities.

**Section\_1: Culture and Leadership**

1. Which of the following do you believe characterises the current position of the Executive and Senior Leadership regarding awareness?
   1. The Executive and Senior Leadership **pro-actively promote a privacy-positive culture and advocate it** as a priority to all levels of the organisation
   2. The Executive and Senior Leadership **pro-actively monitor the promotion** of a privacy-positive culture to all levels of the organisation
   3. The Executive and Senior Leadership **support the promotion** of a privacy-positive culture to all levels of the organisation
   4. The Executive and Senior Leadership **are building awareness** of their role in promoting a privacy-positive culture
2. Which of the following do you believe characterises the current position of the organisation as whole regarding privacy awareness?
   1. Privacy practices and procedures are subject to continuous improvement activities.
   2. Privacy practices and procedures are embedded into business-as-usual processes.
   3. Privacy practices and procedures are available and routinely performed.
   4. Privacy practices and procedures are generally not fully developed, are not fit for purpose or are performed in an ad-hoc manner.
3. Do you follow established, metrics-based privacy reporting processes?
   1. Yes
   2. I am aware of such processes, but not involved in following them
   3. I am not aware of any metric-based privacy reporting processes
4. Are staff sufficiently supported by strong governance structures that support reporting and managing privacy issues?
   1. Yes
   2. No
5. Do existing data governance processes address sensitive and high-risk data?
   1. Yes
   2. No, or I am not involved in data governance processes
6. Do you understand what is meant by a privacy-by-design approach and is such an approach promoted in organisational projects?
   1. Yes
   2. I understand what is meant by privacy by design but am not aware of its promotion in organisational projects
   3. No
7. Are you aware of any ongoing privacy auditing and monitoring processes taking place?
   1. Yes
   2. No
8. Have you provided or been provided with training that ensures staff members are aware of their privacy responsibilities?
   1. Yes, and on a regular basis
   2. Yes, but the training was not regular
   3. No

**Section\_2: Privacy Reporting**

*This section is not applicable to the local government sector*

1. Which of the following best reflects the nature of the statement about privacy compliance included in the organisation’s annual report?
   1. It is subject to routine review and improvement exercises which endeavour to maximise the amount of information provided in the statement, including reflecting the range of privacy response and improvements performed in the reporting period, the privacy priorities of the organisation and how privacy risks and issued are addressed and mitigated against.
   2. It conveys a sense of the nature of privacy management beyond strict compliance and is reflective of the specific privacy management activities carried out by the organisation in the previous year
   3. It is generic in tone, does not change significantly year-to-year, and is designed to be broadly applicable to the privacy management activities carried out by the organisation
   4. A statement is not included in the organisation’s annual report
2. Does the statement include or is otherwise provided alongside statistical details of internal privacy reviews carried out by the organisation in the reporting period?
   1. Yes
   2. No
3. Are the responsibilities and processes around reporting of the statement clearly documented?
   1. Yes
   2. No

**Section\_3: Data Breach Reporting**

1. Is there a process in place to consider and make, if appropriate, a notification of a data breach to IPC NSW?
   1. Yes
   2. No
2. Does the organisation have in place a data breach policy that is accessible to and understood by all staff, and does it identify thresholds for reporting to IPC NSW?
   1. Yes
   2. A policy is in place and accessible to and understood by all staff but it does not identify thresholds for reporting to IPC NSW
   3. No
3. Does the organisation have in place a specific data breach *response plan* that is accessible to and understood by all staff?
   1. Yes
   2. No
4. Is there a prepared communications plan to be followed in the event of a data breach?
   1. Yes
   2. No
5. Does the organisation have in a place an identified data breach response team?
   1. Yes
   2. No
6. Are there processes in place to ensure monitoring of remediation actions subsequent to a breach have been followed and residual risks addressed?
   1. Yes
   2. No
7. Are data breach policies and processes subject to monitoring and improvement activities, regularly and subsequent to each data breach?
   1. Yes
   2. No

**Section\_4: Information Holdings**

1. Which of the following best reflects your understanding of the scope, extent and type of personal information held by the organisation?
   1. The scope, extent and type of personal information and its identification or classification in data management documentation is subject to regular review and acts as in input into wider audit and risk processes
   2. We understand the scope, extent and type of personal information we hold and it is clearly identified and classified as such in data management documentation
   3. We understand the scope, extent and type of personal information we hold but there is no documented data management record
   4. There is not a clear view of the scope, extent and type of the personal information we hold
2. Which of the following best reflects your understanding of the way personal information is stored by the organisation?
   1. The documented view of where and how personal information is stored is subject to regular review, and acts as an input into wider audit and risk processes
   2. We have a documented view of where and how personal information is stored in our organisational systems
   3. We understand the storage arrangements for personal information
   4. There is not a clear view on how personal information is stored
3. Which of the following best reflects your understanding of the purpose for collecting the personal information and what it is used for?
   1. The documented purposes for collection and use of personal information policy are subject to regular review and refined. Risk and audit process include consideration of the purposes for the collection and use of personal information holdings and seek to minimise risk around the holding of personal information.
   2. We have documented the purposes for collecting each piece of personal information and policy which regulates what it is used for and where required, use/provide collection notices
   3. We understand the purpose for collecting the information and what it is used for
   4. There is not a clear view of the purpose for collecting the information and what it is used for
4. Which of the following best reflects your understanding of who has access to the personal information?
   1. The policy which governs access rights, permissions and controls for personal information holdings is regularly reviewed and updated as part of regular systematic privacy and security risk reviews. Physical and system access controls are regularly and procedurally audited to ensure proper application and identify areas for improvement.
   2. We have policy which governs access rights, permissions and controls for personal information holdings, and this is reflected in physical and system access controls
   3. We are aware of the access rights, permissions, and controls for personal information holdings
   4. There is not a clear view of who has access to personal information holdings and the circumstances where access is permitted

**Section\_5: Privacy Impact Assessments**

1. Which of the following best describes how you undertake privacy impact assessments
   1. There is documented guidance provided to project teams that communicate the purpose and process for carrying out a privacy impact assessment. Assessment learnings are incorporated both into the project design as well as more broadly across project teams.
   2. We undertake privacy impact assessments for new projects or where there is a significant change planned, and at a point where outcomes of the assessment can influence project design and development
   3. We undertake privacy impact assessments sporadically or otherwise without a clear understanding of when they should be undertaken
   4. We do not undertake privacy impact assessments,
2. Which of the following best describes how privacy-by-design principles are handled by your organisation?
   1. Privacy by design is adopted and performed by the organisation, supported by guidance, training and project oversight. The application of a privacy by design approach by project teams is subject to monitoring and improvement processes.
   2. Privacy by design principles inform privacy policies and are referenced in guidelines around project design and development
   3. There is awareness of privacy by design and what it intends to achieve in principle, but no application of privacy by design principles in any systematic way
   4. There is little or no awareness of what is meant by privacy by design
3. Do your privacy impact assessments include mapping of information flows, and identification of points where there may be privacy risks?
   1. Yes
   2. No, or else we are not aware that they do
4. Do your privacy impact assessments involve consultations with stakeholders to inform project design
   1. Yes
   2. No, or else we are not aware that they do
5. Do your privacy impact assessments include checks for compliance against the Information Protection Principles and Health Privacy Principles
   1. Yes
   2. No, or else we are not aware that they do
6. Do your privacy impact assessments identify risks and solutions to mitigate the risks identified?
   1. Yes
   2. No, or else we are not aware that they do
7. Are privacy impact assessments treated as a living document, and updated as changes are made to the project?
   1. Yes
   2. No, or else we are not aware that they are
8. Is there a process that leads to privacy impact assessment recommendations being approved by an Audit and Risk Committee where necessary, such as deciding that a project should not go ahead, that changes to the project should occur, that further consultation is required or that the project does not present any privacy risks in its current form?
   1. Yes, and there is evidence of such decisions being made
   2. Yes, but there is no evidence of such decisions being made
   3. No, or else we are not aware of such a process

**Section\_6: Privacy Functions**

1. What best describes the definition of privacy roles and responsibilities?
   1. Delegations and authorisations identified in privacy legislation are understood and defined
   2. Defined delegations and authorisations identified in legislation are not in place
2. What best describes the communication of privacy roles and responsibilities?
   1. Privacy delegations and authorisations are available in writing and are easily located, and staff have a good understanding of these
   2. Privacy delegations and authorisations are available in writing and are easily located
   3. Privacy delegations and authorisations are not well-known, are difficult to access, or are not available in writing
3. What best describes how delegations and authorisations are reviewed?
   1. Delegations and authorisations are subject to regular reviews and are part of a documented process or policy which is carried out as part of any structural changes to the organisation. The outcomes of these reviews seek to identify deficiencies, risks and issues in the oversight of personal information processes.
   2. Delegations and authorisations are subject to regular reviews and are part of a documented process or policy, and there is a record of reviews that have taken place
   3. Delegations and authorisations are reviewed in a sporadic or ad hoc manner
   4. Delegations and authorisations are not reviewed

**Section\_7: Privacy Management Plans**

1. Has your organisation developed a Privacy Management Plan?
   1. Yes
   2. No, or I am not aware of it
2. Has your organisation’s Privacy Management Plan been provided to IPC NSW?
   1. Yes
   2. No, or I am not aware of it being provided
3. Has your organisation reviewed its Privacy Management Plan against the IPC Checklist?
   1. Yes
   2. No, or I am not aware of it
4. Does your Privacy Management Plan include information about how the agency develops policies that deal with compliance under the PPIP Act and HRIP Act?
   1. Yes
   2. No
5. Does your Privacy Management Plan include an overview of the main types of personal information the agency deals with, and how it is relevant to the agency's functions?
   1. Yes
   2. No
6. Does your Privacy Management Plan include strategies in place to comply with the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs)?
   1. Yes
   2. No
7. Does your Privacy Management Plan include any exemptions to the PPIP Act or HRIP Act?
   1. Yes
   2. No
8. Does your Privacy Management Plan include details of any public registers?
   1. Yes
   2. No
9. Does your Privacy Management Plan include details of strategies to minimise the risk of employees committing an offence?
   1. Yes
   2. No
10. Does your Privacy Management Plan include procedures for privacy internal reviews?
    1. Yes
    2. No
11. Does your Privacy Management Plan include an approach to training staff in the agency about privacy requirements, policies and practices?
    1. Yes
    2. No
12. Does your Privacy Management Plan include references to relevant policies such as record keeping policies?
    1. Yes
    2. No
13. Is the Privacy Management Plan easily accessible on the agency website and made available in other ways on request?
    1. Yes
    2. No
14. Do you have a process in place to review and update the plan?
    1. Yes, at least annually
    2. Yes
    3. No

**Section\_8: Internal Reviews**

1. Does your agency have a process to notify the Privacy Commissioner that an application for internal review has been received?
   1. Yes
   2. No
2. Are reviews undertaken by an individual within the agency who is directed by the agency to deal with the application, is suitably qualified to deal with the subject of the complaint, and was not involved in any way in the original matter?
   1. Yes
   2. No
3. Are reviews completed within 60 days from the date the application was received?
   1. Yes, and there is oversight in place to monitor and ensure completion of the review well within legislative requirements
   2. Yes, but no formal oversight processes are in place
   3. No
4. Are there processes in place to ensure that the Privacy Commissioner is given an opportunity to review the draft findings and make any submissions as necessary within those 60 days?
   1. Yes
   2. No
5. Are there processes in place to ensure that the Applicant is informed of their right to seek administrative review at NCAT if not completed within 60 days?
   1. Yes,
   2. No
6. Do reviews identify remedial actions that should be implemented, and monitor to ensure that these occur? Remedial actions might include for example, staff training, updating relevant policies and providing an apology
   1. Yes
   2. No
7. Are applicants notified within 14 days of completion of the review of the findings of the review, the actions proposed to be taken and the right of the individual to have the findings reviewed by the Tribunal?
   1. Yes, and there is oversight in place to monitor and notification to the applicant occurs well within legislative requirements
   2. Yes, but no formal oversight processes are in place
   3. No
8. Are there processes to ensure that the Privacy Commissioner has been notified of the findings of the review and the actions proposed to be taken?
   1. Yes
   2. No