information and privacy commission new south wales

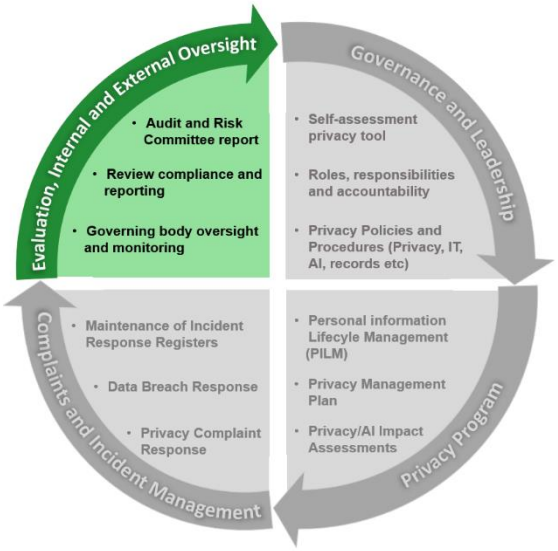
Privacy Governance Framework

February 2024

Evaluation, internal and external oversight

Evaluation, auditing and reporting

Agencies should ensure that there are adequate processes in place to track and measure privacy performance. The identifiable privacy performance measures should then be reported to the agency leadership in accordance with the agency's risk management processes. Auditing and risk functions should ensure that privacy is part of the audit process within the agency, ensuring that its policies and processes are regularly reviewed, up to date, and fit for purpose. Additionally, agencies need to ensure they comply with regulatory oversight and NSW Government accountability mechanisms.



Agencies should have in place metrics and processes in place to collect data to track privacy management and the maturity of their privacy program over time. This can help support business cases for additional resourcing, demonstrate improved privacy maturity and/or show areas of weakness and opportunity. Importantly, it can also assist in building the overall operational resiliency of the agency.

Checklist

- Is data captured to assess privacy requests or complaint responses? If not, what metrics are appropriate to put in place? For example: the average length of time taken to respond to a privacy request, or the average length of time to carry out an internal privacy review.
- Is the organisation pro-actively examining the privacy implications, risks and benefits of new technologies it introduces into the organisation and have a process for addressing identified risks.
- Are organisational risk registers regularly reviewed to ensure privacy risks are being appropriately managed?
- Is your agency collecting data on personal information lifecycle management? For example, are systems being reviewed and measured:
    - to assess whether all of the personal information being collected is necessary, or
    - to ensure and record active disposal of personal information when it is no longer required to be retained?
- Is data being collected in relation to privacy training and awareness initiatives, and is it being included in your agency's overall privacy reporting?
- Is data being collected on privacy impact assessments (PIAs)? In particular, whether risk mitigation measures documented in the PIA have been carried out and whether any requirements for periodic reviews have been done, as required by a PIA.
- Are data breach incidents and reporting being included in your agency's overall privacy reporting?
- Following a data breach, and the investigation that the agency is required to carry out in 5.5.1 of the Guide to managing data breaches in accordance with the PPIP Act (i.e. to investigate what went wrong and to update relevant policies and procedures to remedy any issues to prevent future breaches), have the agreed remediation actions arising from the post-incident review been carried out and documented in the Privacy Management Plan?

What are the oversight and accountability mechanisms?

The PPIP Act and the HRIP Act make public sector agencies accountable for the way they handle personal information and health information and records, including sharing information with a third party.

These mechanisms include:

- The Privacy Commissioner's oversight role.
- Parliamentary oversight of the Privacy Commissioner via the Committee on the Ombudsman, the Law Enforcement Conduct Commission and the Crime Commission (OmboLECC).
- The NSW Civil and Administrative Tribunal who provide individuals with a channel for review and potential redress if their privacy concerns are unresolved.

Further mechanisms available under the HRIP Act include the ability to refer complaints, where appropriate, to the Health Care Complaints Commission and the Commonwealth Privacy Commissioner.

- *Annual Reports (Departments) Regulation 2010*
- *Annual Reports (Statutory Bodies) Regulation 2010*