New Zealand Government

Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 2.0)

Internal Affairs
Te Tari Taiwhenua

The Department of Internal Affairs Te Tari Taiwhenua would like to acknowledge and thank KPMG for their assistance in developing the Privacy Maturity Assessment Framework, assessment tool, and user guide, and Statistics New Zealand for leading the development of version 1.0.

Citation
The Department of Internal Affairs Te Tari Taiwhenua (2014). *Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 2.0)*. Published by Department of Internal Affairs on behalf of the New Zealand Government. Available from https://psi.govt.nz/privacyleadership/.

To be read in conjunction with *User guide for the Privacy Maturity Assessment Framework (version 2.0)* and the Privacy Maturity Assessment Tool, which are both available on the Privacy Leadership Toolkit on the Public Sector Intranet: https://psi.govt.nz/privacyleadership/.

Published in July 2014 by
The Department of Internal Affairs Te Tari Taiwhenua on behalf of the New Zealand Government
Wellington, New Zealand

Contact
Government Chief Privacy Officer, Department of Internal Affairs
gcpo@dia.govt.nz

Introduction

The purpose of this document is to provide details of the elements, attributes, and criteria of the Privacy Maturity Assessment Framework.

The Privacy Maturity Assessment Framework enables agencies to assess and improve their privacy practices. It consists of nine elements that provide criteria against which an agency can assess their privacy maturity. Maturity is assessed through five possible maturity levels.

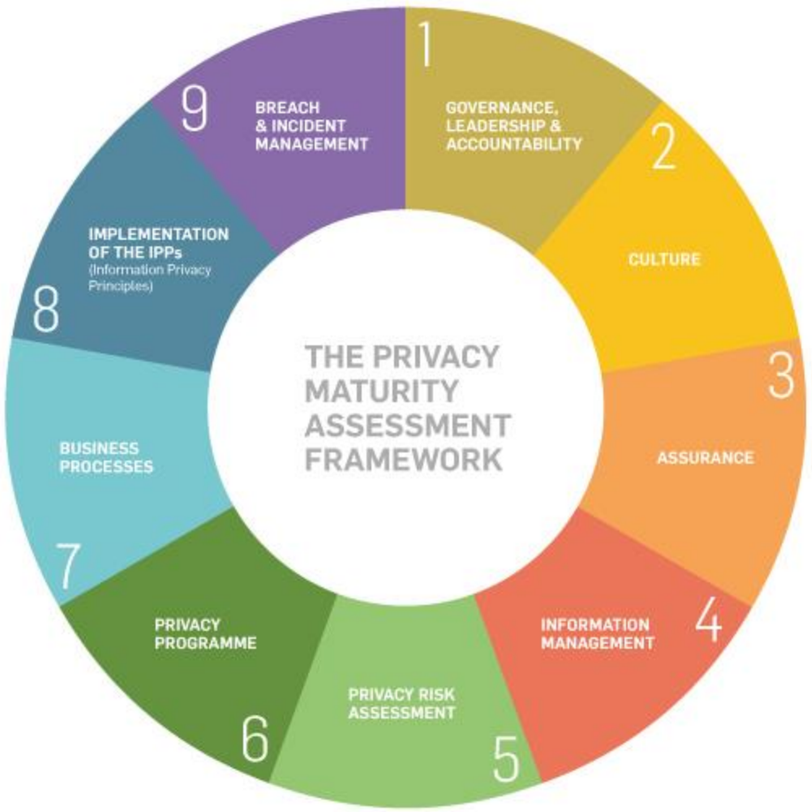
You can access the Privacy Maturity Assessment Framework on the Privacy Leadership Toolkit on the Public Sector Intranet (available to subscribed public sector agencies).

The framework was tested during a pilot phase with a number of public sector participants between October 2013 and March 2014. Subsequently, updates to reflect the results of the pilot were made to the framework and guidance.

Read this document in conjunction with:

- *User guide for the Privacy Maturity Assessment Framework (version 2.0)*
- Privacy Maturity Assessment Tool, which is an Excel tool for recording ratings and providing visual summaries.

See the figure below for a visual representation of the elements of the Privacy Maturity Assessment Framework.



Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 1.0)

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
1	**Governance, leadership, and accountability**	**Senior leadership commitment**	Leadership commitment for comprehensive privacy management is not demonstrated. No support for or awareness of privacy initiatives. The privacy programme of work is not adequately resourced.	Leadership considers privacy as issues or breaches arise. Managers are aware of privacy initiatives within their business units. Management is aware of the resources and core skills needed to effectively deliver a privacy programme of work, but further resourcing is required.	Leadership is aware of the agency's privacy management and actively promotes it e.g. through information available on the agency's intranet, or regular agency-wide communications. Dedicated resources are allocated to deliver the privacy programme of work.	Leadership takes a proactive and integrated approach to leading privacy management. Resourcing for privacy is considered at a strategic level within the agency.	Leadership works collectively to seek innovative ways to continuously improve privacy management. Resources are deployed strategically to support the ongoing integration of the privacy framework into the business strategy. Information obtained through risk assessment or review of response to any identified breach is used to inform deployment of resources.
		Governance oversight	Limited or no reporting and access to the governance board /committee(s) / executive leadership team.	Established reporting lines to the governance board / committee(s), and access to the executive leadership team exist, but these are used largely in response to specific issues. Discussions on privacy are included in governance board / committee(s) / executive leadership team meetings, but these are largely in response to specific issues.	Governance board / committee(s) / executive leadership team receive regular updates on the privacy programme. Governance meetings include discussions on privacy issues and the effectiveness of the privacy programme.	Management proactively reports to the governance board / committee(s) / executive leadership team, to inform them of significant changes to the privacy risk profile. Governance meetings include discussions on the strategic direction of the privacy programme and privacy as an integral aspect of risk management.	Functional oversight of the privacy function and programme is included in the risk management organisational structure and is shown by setting policies and monitoring compliance. The governance board / committee(s) / executive leadership team actively informs business performance and improvements on privacy management.
		Management structure, roles, and responsibilities	Limited or no defined reporting structures for privacy management, issues, or improvement. No senior executive responsible for privacy management.	Some existing line management and reporting structures are in place for privacy management, issues, and improvement. A senior executive is formally responsible for privacy management, but has limited oversight or involvement in the privacy programme.	Formal and structured line management and governance over privacy management exists. There is formal responsibility and accountability for each element of the privacy programme and for the implementation of the Information Privacy Principles into the business. A senior executive is authorised to make decisions on privacy management, including the programme's content, approach, and resourcing. This person is accountable for privacy management and maintains oversight of the agency's privacy management.	Governance board / committee(s) / executive leadership team has a governance role in privacy (ie strategic decision-making and approval of policy) rather than undertaking day-to-day management of the programme. Senior management views privacy assessment and management as integral to their role.	Ongoing, regular, and formal discussions on privacy occur between the governance board / committee(s), and the executive management and senior management levels. A formal privacy management structure covering the entire agency is in place.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
		Privacy officer	Non-existent or undocumented privacy officer role, and undefined privacy leadership structure. No centralised oversight or specific accountability for ensuring the privacy principles are adhered to. Where a privacy management function exists, communication between the privacy officer / privacy management function and other parts of the agency is limited.	Privacy officer / privacy management function responsibilities are documented and the role is known throughout the agency. Privacy officer's role mainly consists of meeting the requirements of the Privacy Act 1993, eg dealing with privacy disclosures and complaints. Communication between privacy officer and other parts of the agency largely occurs in response to breaches.	Privacy officer / privacy management function oversees a privacy work programme and maintains central oversight of privacy initiatives and activities on an agency-wide basis. Privacy officer / privacy management function communicates regularly with other 'second-line-of-defence' functions (eg records management, security, risk management).	Privacy officer / privacy management function contributes to business process design and risk assessment. Privacy officer / privacy management function has established ongoing communication and clear alignment (where applicable) with the work programmes of other second-line-of-defence functions.	Privacy officer / privacy management function is responsible for the operational and strategic elements of privacy management on an agency-wide basis. It also has the capability, capacity, and authority to introduce and implement privacy management better practices. Second-line-of-defence function proactively approaches the privacy function for input to their work programmes. This communication is open, honest, and ongoing.
		Privacy strategy	No consideration for or integration of privacy management in strategy planning. No defined tolerance levels in relation to individual privacy risks. No consideration for privacy strategy by the governance board and/or committee(s), and/or the executive leadership team.	Privacy strategy and management programmes are in place, including consideration of the corporate level risk appetite. No meaningful definition of privacy risk appetite other than what is set as the corporate strategy. Privacy strategy is considered and approved by the governance board / committee(s) / executive leadership team.	Privacy strategy and management programme are reviewed and revised regularly to confirm their ongoing suitability with the internal and external environments (including regulatory requirements). Defined privacy risk appetite exists, which is used to assess resource requirements and timelines for dealing with privacy risks at an operational level. Privacy strategy formally adopted by the governance board / committee(s) / executive leadership team exists.	Results of privacy risk assessments are used to inform and update the privacy strategy and plan. Governance board / committee(s) / executive leadership team know what risk appetite means in relation to privacy and to the objectives and strategies set by executive management.	Privacy considerations are integrated into the overall business strategy, with risk appetite considered in future strategic options. Context for setting the privacy risk appetite is clearly defined and understood by the governance board / committee(s) / executive leadership team. The context includes external and internal trends and expectations. Privacy risk appetite is regularly reviewed, taking into account this context. Information obtained through risk assessment or review of response to any identified breach is used to inform updates to the privacy strategy.
		Accountability	Unclear or undocumented accountability for privacy management.	Privacy management is allocated to specialist individuals who are seen as accountable for privacy management within siloed areas of the agency. While the role may be included in a person's job description, it is only considered meaningful when a significant breach is identified.	Accountability of individual employees in relation to privacy management is documented, known, and accepted. Processes are in place to evaluate staff performance against defined and communicated expectations.	All staff and contractors are responsible for ensuring the principles of privacy management are adhered to. This responsibility is an integral part of their performance assessment and management.	All staff and contractors are responsible for privacy management and consider it normal practice to identify opportunities for improvement.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
2	**Culture**	**'Tone at the top'**	Limited or no behavioural modelling by senior management of the agency's privacy values, or no defined values. No support or encouragement for staff to properly implement privacy-focused practices. No active promotion or culture of reporting privacy breaches. Privacy breaches are largely discovered by external parties (eg media or inadvertent recipient of personal information).	Senior management recognises the need and importance of establishing and maintaining an ethical culture but are inconsistent in their approach to developing this. The principles they aspire to are documented but not incorporated into business processes. Staff are encouraged to report privacy breaches relating to inappropriate disclosure of personal information to a third party. The level of comfort staff have with reporting incidents varies between divisions.	Senior management actively and visibly demonstrate commitment to promoting good privacy practices for themselves, their peers, and their staff. A clear articulated privacy vision or privacy policy statement exists of which everyone is aware of, senior managers visibly support, and all managers use. Staff are encouraged to report privacy breaches and incidents relating to the 12 Information Privacy Principles, and are comfortable doing this.	Senior management and governing bodies work together and with their teams to visibly deliver consistent, positive messages on how the agency views, manages, and deals with privacy. Everyone understands the privacy policy statement and accepts that it shapes their behaviour. Management is confident that all privacy incidents, breaches, and complaints are escalated and reported within required timeframes.	Leadership work collectively and visibly to seek innovative ways to continuously improve privacy management. Managers and leaders are committed to making privacy core to the culture through their visible actions, planning, and decision making. Everyone believes and is committed to it, regarding it as a personal value with their daily actions reflecting this commitment. Staff and management are comfortable identifying areas for improving privacy practices and discuss/raise these freely and proactively.
		Respect for privacy – customer focused culture	No formal documentation or guidance on why privacy is important and what it means, in practice and principle, to individuals and the agency.	No connection between the value system of the agency and behaviour displayed by staff. Privacy management is almost exclusively a focus area of specialists.	Defined values and aspirations in managing privacy are communicated in clear terms and are consistently understood throughout the agency. The Agency's privacy expectations are clear to staff.	Personal information is considered as important and belonging to the individual. Privacy is integrated into business processes to improve practices, customer relationship management, and reputation.	Everyone in the agency actively identifies with and aligns to the privacy mission of the organisation; transparency and accountability are the norm; new insights are acted upon in unison; and conflicts are resolved positively and effectively. Central to the agency's culture and approach is everyone taking responsibility and accountability for ensuring personal information is treated appropriately and with respect.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
3	**Assurance**	**Assurance model**	Limited ad hoc assurance activities occur in response to breaches. No formal, planned programme of assurance across the first (business operations), second (oversight functions), and third (independent assurance) lines.	Limited assurance is undertaken over the privacy management framework and underlying processes and controls. First line: Privacy controls are built into business processes in response to breaches. Second line: Privacy function's oversight activities are largely in response to specific breaches. Third line: Internal audit largely provides assurance activities in response to specific breaches.	Defined programme of assurance for privacy across the agency. First line: Links between operational privacy risks identified in the agency's risk registers and the agency's control activities are documented. Second line: The privacy function and other second-line functions (eg records management, security, risk management) are responsible for providing oversight of the agency's privacy management practices. Third line: Internal audit (or other equivalent independent assurance function) conducts regular privacy-related assurance activities.	The three lines of assurance approach are adopted for privacy; with the privacy function/risk function operated primarily as second-line assurance (ie with a focus on oversight of the agency's privacy management practices). First line: Business processes are designed to mitigate residual privacy risk to within the agency's risk tolerance. Second line: Privacy function and other second-line functions provide oversight and look for opportunities to continuously improve the agency's privacy management. Third line: Internal audit uses the privacy risk management output, at a strategic and operational level, in their audit planning.	The three lines of assurance approach are firmly in place, with each line providing ongoing feedback on the effectiveness of privacy management and the system of internal control over privacy. First line: The business continually identifies risk and business improvement actions and implements effective controls. Second line: Privacy and risk activities are integrated with the wider system of internal control as part of an efficient, effective assurance framework. Third line: Internal audit has a systemic and disciplined approach to evaluate and improve the agency's privacy risk management, control, and governance processes.
		Monitoring and reporting	No structured or formal monitoring and reporting lines for privacy assurance.	No formally defined privacy assurance monitoring in place. Reporting lines are only used as issues arise. Performance of the agency's privacy programme is informally monitored.	Regular assurance activities, with defined monitoring and reporting requirements, assess the performance of the elements of the privacy framework. Reporting lines are clearly defined. Agency's privacy-related key performance indicators are used to track and measure the performance of the privacy function. Performance is regularly reported to management.	Outcomes of the assurance programme are used to inform changes to the processes and responsibilities for managing personal information. Key performance indicators for the agency's privacy programme and privacy management are established in the context of the privacy strategy. These indicators are proactively communicated to management and improvements to the privacy programme made where gaps are identified.	Outcomes of the assurance programme are used to inform changes to the agency's privacy risk management, control, and governance processes. Reporting is formal and sent to all appropriate levels of the business including senior managers. The agency's privacy key performance indicators are used to track and measure organisation-wide privacy performance. These indicators are used to drive all aspects of organisational privacy management improvement.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
4	**Information management**	**Principles for managing data and information**	No formal documentation or guidance clarifying the principles for managing information.	Awareness exists at management level of how to properly manage information and/or documented policies or processes. However, there is no implemented programme(s) or resourcing to effectively manage information.	Information management principles and associated policies are in place. Defined principles include: • Information is managed throughout its life-cycle, including long-term preservation and access and caters for technological obsolescence. • Collaboration with other agencies and the public, facilitating access, strengthening awareness, and supporting international collaboration. • Data and information support the purposes for which they were collected • Information is only collected for specified public policy, operational business, or legislative purposes. • Data and information are accurate, relevant, timely, consistent, and without bias in that context. • Personal, confidential and classified data and information are protected. Staff apply these principles as part of business-as-usual.	Staff and management proactively contribute to the continuous improvement of practices in place to support and complement the information management principles and associated policies. They identify and communicate gaps and opportunities for improvement.	A formal information management structure covering the entire agency is in place. This structure is actively supported by all management and staff.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
		Information management strategy	No consideration for or integration of information management in strategy planning. Tolerance levels in relation to individual information management risks are not specified. No consideration for information management strategy by the governance board / committee(s) / executive leadership team.	Information management strategy has been developed and approved, including consideration of the agency's risk appetite. No meaningful definition of information risk appetite exists other than in the corporate strategy.	Regular review and revision of information management strategy and programme to confirm their suitability with the internal and external environment (including regulatory requirements). Defined information management risk appetite is used to assess resource requirements and timelines, which deal with information management risks at an operational level. Information management strategy formally adopted by the governance board / committee(s) / the executive leadership team.	Results of information risk assessments are used to inform and update the information management strategy and programme. Governance board and/or committee(s), and/or the executive leadership team know what risk appetite means in relation to information management and to the objectives and strategies set by executive management.	Information management considerations are integrated into the overall business strategy, with risk appetite considered in decisions around future strategic options. The context for setting the information management risk appetite is clearly defined and understood by the governance board / committee(s) / the executive leadership team.This context includes consideration of external and internal trends and expectations. The information management risk appetite is regularly reviewed, taking into account this context.
		Information management business processes	Processes and controls may not be formal, documented, or consistent. No effective process to ensure that changes to business processes, or that new business processes, are assessed for their impact on information management requirements. Existing information management processes do not specifically address privacy risks or management. Information is shared with other agencies without explicit consideration of privacy implications.	Implications of ineffective information management processes are only realised when privacy breaches or other issues occur. Remedial action is either system or business unit specific. Informal processes for dealing with requests to share personal information with other agencies are in place. These processes consider the privacy risks if information is to be shared with other agencies. In some cases, processes include documented agreements between agencies.	Personal information and privacy management is part of overall information management processes. Personal information considerations are included in the IT strategy. Personal information shared with other agencies is subject to documented agreements that comply with relevant legislative requirements, including the Privacy Act 1993. Before information is shared, it is reviewed to ensure privacy implications are considered.	Personal information and privacy management is integrated into business processes and is considered when changing or collecting new data. Emerging risks on information management are reviewed by management and changes are made proactively to policies and procedures as required. Training is developed / revised in response to these risks. Information, including personal information, is managed as an enterprise asset. Well-developed organisation and governance processes and organisational structures exist.	Personal information and privacy management is a strategic initiative. Issues are either prevented or corrected at the source, and best practice architecture is implemented. Information obtained through risk assessment or review of response to any identified breach is used to inform updates to information management business processes and design.There is a strong focus on continual improvement.
5	**Privacy risk assessment**	**Integration with enterprise risk management**	No relationship between privacy function and wider risk-management function.	Limited interaction between the privacy function and the risk function to mitigate specific identified risks (i.e. conversations only take place to identify future risks based on existing issues identified)	Privacy risk assessment processes generally align with the agency's risk-management approach.	Privacy risks are considered within the agency's enterprise risk management programme. Privacy risks and issues are owned by the business units.	Considerations of privacy risk are firmly in place within the agency's enterprise risk management function. The risk management function considers privacy risk identification as a business-as-usual activity.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
		Risk identification and assessment	No formal, structured, or consistent process for identifying and assessing privacy risks.	Incomplete or underdeveloped processes for privacy risk identification. Privacy risk management is issues-based. Regular or occasional risk identification and assessment is performed.	Privacy risk identification and assessment occur on a regular basis. However, these are often viewed as a compliance-based activity.	Proactive identification and assessment of privacy risks before issues occur, which most management and staff perceive as adding value.	Well defined, highly evolved, and efficient risk identification processes are in place, which are integrated into business activities across the agency. All management and staff believe these processes add value to the agency.
		Privacy risk monitoring and reporting	No formal process for monitoring privacy risks. No formal process for reporting on privacy risks and mitigations.	Privacy risks are monitored on a siloed basis in business lines, with little if any cross-functional interaction. Privacy risk reporting is largely by exception and in response to identified issues.	Privacy risks are monitored mainly on an operational level, with some information held at a central level regarding external trends and emerging risk areas. Agency reports on privacy risks proactively.	Monitoring includes analysing key privacy risks; whether risk levels have changed, controls are applied appropriately, and risk management improvement requirements are being implemented. Defined risk management reporting requirements in place, integrated with business-as-usual management reporting.	Analysis / monitoring of privacy risk information is conducted to review the trends from historic information and the effectiveness of controls. The privacy function supports the agency in improving controls and implementing best privacy management practice. Reporting on privacy risks includes the key risk indicators. Risks are linked to the privacy strategy and key performance indicators, so that risk information is integrated into reporting on privacy management performance.
6	**Privacy programme**	**Programme of work**	Agency knows it needs to improve its privacy management, although is doing little to address this.	Risk and outcomes drive the privacy work programme to varying levels within business units / divisions. Agency is able to address some of its privacy issues. However, this does not happen until after issues have occurred.	Risk and outcomes drive the privacy work programme across the agency. Agency uses root cause analysis to address systematic and systemic privacy issues.	Privacy programme results in proactive identification and resolution of potential privacy issues and risks, education to improve compliance with the principles of the Privacy Act 1993, and strategies for assessing and improving privacy management.	An effective process is in place to ensure that any changes to privacy obligations or best practice are identified and practices are updated to reflect these across the agency. Privacy is treated as a core competency across strategy, people, process, technology, and controls. Information obtained through risk assessment or review of response to any identified breach is used to inform the privacy programme of work.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
		Privacy policies and procedures	No identifiable privacy management policies and procedures.	Staff are aware of policies and procedures but these are not consistently followed and may not be comprehensive. Non-compliance is not identified. Inconsistent or incomplete reviews and comparisons of privacy policies and practices with applicable laws and regulations.	Easy-to-understand and relevant policies and procedures are in place, resulting in a common approach to privacy management across the agency. Privacy policies and procedures are reviewed to ensure their compliance with applicable laws and regulations, and other environmental requirements or impacts, in response to identified privacy breaches.	Staff and management proactively contribute to designing practices to support and complement privacy policies. They identify and communicate when gaps and opportunities are identified. Management proactively reviews changes to privacy legislation, regulations, and emerging risks, and amend their agency's privacy policies and procedures as required.	The required behaviours and principles of the privacy policies and procedures are consistently demonstrated by employees and management as business-as-usual. An effective process is in place to ensure that any changes to best practice, including information obtained through risk assessment or review of response to any identified breach,are identified and reflected in privacy policies/procedures.
		Privacy training and awareness	Limited or no privacy training available to staff. Staff/contractors have limited or no awareness of privacy requirements. Limited or no processes to detect gaps in staff/contractors' understanding of the privacy programme.	Agency has compliance-based privacy training, completed within divisions with little central oversight. Awareness of privacy principles is limited to preventing disclosure of personal information to external parties. Any lack of staff/contractor understanding may only be identified when incidents/breaches occur.	All staff/contractors are required to undertake basic privacy training, with more practical job-based training within divisions on a needs analysis basis. Training is adequate in content, frequency, and form. Staff/contractors are aware of the privacy principles, privacy policies, and other privacy management resources available to them. Staff/contractor understanding and awareness of privacy requirements is monitored and training given where gaps are identified.	The privacy understanding of new staff/contractors is assessed before they are given access to particularly sensitive personal information (eg health information). All staff/contractors are aware of the requirements of the Privacy Act 1993 and how these apply to their jobs. Training is developed/revised in response to emerging privacy risks identified.	Privacy training empowers all staff/contractors to feel confident in their approach to managing personal information. Their understanding of privacy is assessed as sufficient before dealing with all types of personal information. All staff/contractors are active in identifying privacy risks, control gaps, remediation, and improvement opportunities. Training is revised to align with best practice and continuously stimulate employees. It is role-specific. Information obtained through risk assessment or review of response to any identified breach is used to inform training needs.
		Internal communication	No formal privacy management communication systems or processes in place to communicate key decisions and messages. Business units do not seek specialist guidance on privacy management activities.	Privacy management communication systems exist. However, these are not formally defined. Communication is primarily one-way (top-down).	Clear privacy management communication protocols are in place, which are demonstrated through privacy/risk forums and team meetings. Two-way communication between staff and management is actively encouraged.	Two-way open privacy management communications are used and processes are in place to ensure key messages are received and understood by staff/contractors within the agency.	Clear, frequent communication occurs between governing bodies, the agency, as well as across functional bodies about privacy management and the effectiveness of existing initiatives. Learnings are readily shared among business units to ensure best privacy management practices are consistent across the agency.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
7	**Business processes**	**Personal information inventory and classification**	No clear strategy for identifying and managing personal information held by the agency.	Separate parts of the agency are aware of the personal information they hold or have access to and may have made attempts to define, document, or classify this. However, there is no organisation-wide assessment or knowledge of what personal information is held.	There is an effective, centralised process for identifying, classifying, and documenting all personal information collected, used, shared, or accessed by the agency. Complete inventory of personal information held exists. The value of information held (ie, quantity, quality, sensitivity, etc) is taken into account when planning appropriate actions to mitigate privacy risks.	Personal information is identified, classified, and documented as part of the wider information management system. There are documented data flows of personal information collected, used, stored, and disclosed for key processes.	All personal information, how it is collected, secured, accessed, corrected, stored, disclosed, used, and classified is recorded and regularly assessed. There are documented data flows of personal information collected, used, stored, and disclosed for all processes.
		Privacy analysis integrated into Policy Advice to Ministers	No formal process for ensuring privacy risks and issues are considered when providing Policy Advice to Ministers.	Privacy risks and issues are sometimes considered when providing Policy Advice to Ministers but no compulsory or formal process exists.	There are documented requirements to consider privacy risks and issues when providing Policy Advice to Ministers.	Privacy analyses actively seek to identify ‘win-win’ policy solutions (ie Policy outcomes are consistent with the desired privacy outcomes).	The effectiveness of Policy Analysis in achieving desired privacy outcomes is reviewed and changes made as a result if the outcomes are not satisfactory.
		Privacy management designed into business processes	No formal process for ensuring privacy risks and issues are considered when designing/reviewing business processes.	Privacy risks and issues are sometimes considered when designing/redesigning key business processes and systems. However, this is not compulsory.	There are documented requirements to consider privacy risks and issues in the design phase for all processes and systems.	Business processes are designed specifically to reduce privacy-related risks, with privacy considerations embedded into change-management processes.	All business processes are designed with ‘privacy as the default setting’. Business processes are proactively updated throughout the agency to reflect changes in best practice for privacy management due to: emerging risks, information obtained through risk assessment or review of response to any identified breach, and changes to legislative/regulatory requirements. New business processes are developed where needed.
		Privacy impact assessments	No effective process is in place to ensure that new or revised business processes are assessed for their impact on privacy management requirements.	Informal, little known, or inconsistent process is in place for considering how new business processes or changes to existing ones will affect privacy management.	Formal, documented, and effective processes are in place to ensure that changes to business processes, or new business processes, are assessed for their impact on privacy management requirements. Documented systems-development and change-management process in place that includes a privacy impact assessment for all technology, tools, and business process changes to personal information collected, used, shared, or accessed by the agency.	Privacy impact assessments are independently reviewed when appropriate, based on a mature understanding of risk, to ensure the review was effective and results properly implemented. Recommendations from the independent review are implemented where necessary.	Privacy impact assessments are centrally referenced so that subsequent change can build on earlier analysis. Privacy impact assessments are also applied to existing business processes to identify opportunities for improvement.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
		Third party contracts and relationships	Limited due diligence is undertaken over third parties' privacy policies, practices, and procedures.	Level of due diligence undertaken on third parties' privacy, policies, practices, and procedures varies between business units and may only occur in response to a breach. Third party contracts include a confidentiality clause.	Where third parties have access to personal information, due diligence is performed and assurance sought over their privacy and security practices and policies. Due diligence includes developing an understanding of what personal information will be held and what it will be used for. Contract templates include a standard privacy clause that covers the treatment of personal information. Third parties with access to personal information are educated about incident response and escalation processes.	Contract terms and conditions vary depending on the nature, volume, and sensitivity of the personal information the third party has access to. Contracts are made with third parties only if their level of protecting personal information is comparable to the agency. Third parties are regularly reviewed against the requirements of their contracts.	A privacy risk assessment for third parties is completed before any contract under which personal information is made available is granted. Privacy audits of third parties are undertaken on a regular basis and they are held accountable for the results. Issues and/or emerging risks relating to contracting and contract management processes are analysed. Mitigation strategies are put in place to improve existing and future contracts where third parties have access to, use, collect, or disclose personal information.
		Control activities	Limited or no controls are designed or implemented specifically to mitigate privacy risks (eg preventative controls to prevent a breach or incident occurring, or detective controls to identify breaches or incidents quickly).	Control activities that respond to identified privacy risks exist. However, these are not formally documented. Requirements or processes for monitoring and reporting of privacy controls are not fully documented.	There are documented systems of internal controls, which mitigate controllable privacy risks to an acceptable level given the agency's risk tolerance. Controls selected for monitoring and the frequency with which they are monitored are based on a risk assessment.	Privacy risk mitigation plans are applied and integrated across the agency. The privacy function coordinates these plans and ensures mitigations are applied consistently across different business areas affected by the same risks. Management is responsible for reviewing privacy controls and their effectiveness, and reports on this review with evidence of improvement. This is seen as part of their formal roles and responsibilities.	Continuous auditing/monitoring occurs to detect, monitor, and prevent control breakdowns in key/high-risk systems that contain personal information. The agency tracks the implementation and effectiveness of key privacy controls and works closely with central functions and external reviewers to optimise privacy risk management and control.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
8	**Implementation of the Information Privacy Principles (IPPs)**	**IPPs 1–4: Collection**	No formal, documented, or consistent processes to ensure that information is only collected as necessary for the purposes identified. No formal, consistent controls for ensuring individuals are notified when their personal information is collected.	Some documented procedures are in place for identifying personal information, but the agency does not obtain evidence to show they have identified all of it. Agency has basic understanding of what personal information is being (or has been) collected, why it is collected, and where it is kept. (i.e. a formal & comprehensive personal information inventory has not been undertaken)	Documented and complete policies and processes in place to: • distinguish the personal information that is necessary for the purposes identified • differentiate the personal information necessary for the purposes identified from optional information • limit collection to information necessary for the purposes identified • notify individuals about all relevant privacy policies at or before collection • provide information about the consequences of refusing to provide personal information or denying or withdrawing consent. Assurance/evidence is obtained to demonstrate compliance with/effectiveness of these policies and processes, or there is a plan in place to obtain this assurance/evidence.	Documented and complete policies and processes are in place to: • regularly review the need for personal information to be held • clarify the consequences, if any, to individuals of refusing to provide requested information and indicate that certain information may be developed about individuals • regularly review these consequences to ensure they are complete, accurate, and relevant. Assurance/evidence is obtained to demonstrate compliance with/effectiveness of these policies and principles and to identify exceptions.	Documented and complete policies and processes are in place to ensure: • changes in the need for personal information are proactively identified, leading to changes to the relevant business processes and policies • unnecessary collection of information is proactively identified • corrective action is taken when the information collected is not necessary for the purposes identified • process updates and improvements are made when feedback is provided • the consequences of denying consent are reduced. Assurance/evidence is obtained to demonstrate compliance with/effectiveness of these policies and principles.
		IPP 5: Security	No formal, consistent, privacy-focused controls over systems and physical storage mechanisms containing personal information.	Standard security procedures exist, but these are not specific to the control of personal information and so may not be appropriate. Security measures are informally linked to sensitivity of personal information held or to business need, as perceived by staff (ie level of sensitivity not formally approved by management).	Documented and complete processes in place to controlaccess to personal information Security levels are formally linked to a demonstrated business need to access personal information. Assurance/evidence is obtained to demonstrate compliance with the principles around security, or there is a plan in place to obtain this assurance/evidence.	Processes are in place to detect and monitor inappropriate access to hard-copy files, databases, and other resources containing personal information. Access rights are updated when staff change jobs, leave the agency, or when systems change. A review of security measures is included as a requirement in change processes and in processes implemented when new types of personal information are obtained or used by the agency. Assurance/evidence is obtained to demonstrate compliance with security principles and to identify exceptions.	Automated processes are in place to continuously detect and monitor irregular access of authorised personnel and logical access controls. Ongoing assessment of security measures over personal information exists.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
		IPP 6: Access	Informal, undocumented, and inconsistent processes for: • ensuring an individual is able to request access to their personal information • ensuring their identity is verified • monitoring requests for access • recording requests and timeliness of responses • reporting on requests.	Some documented procedures on how people can access their personal information and verify their identity, but the agency does not obtain evidence to show these are always applied and are effective.	Documented and complete policies and processes in place to: • ensure an individual can request confirmation that personal information is held and have access to it • monitor information and access requests to ensure appropriate access is provided • ensure individuals are authenticated before granting them access to personal information. Processes to verify identity are documented, understood, and consistently applied. Assurance/evidence is obtained to demonstrate compliance with the principles around access (ie sufficient controls are in place to ensure all the personal information held on an individual is identified and provided when requested, and to verify that this is the case) or a plan is in place to obtain this assurance/evidence.	Processes are in place to: • identify ways of improving efficiency and completeness of searching for personal information • review the validity of granting requested access. Assurance/evidence is obtained to demonstrate compliance with access principles and to identify exceptions.	All complaints and/or concerns relating to access of information are reviewed and improvement opportunities identified and implemented as a result. Access to personal information is through self-service when possible and appropriate.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
		IPP 7: Correction	Informal, undocumented, inconsistent processes and controls for: • ensuring an individual is able to correct personal information • ensuring the statement of correction is attached to the personal information when appropriate • monitoring requests for correction • recording requests and timeliness of responses • reporting on requests.	Some documented procedures for updating or correcting personal information, for validating requests, and for informing third parties where relevant, but the agency does not obtain evidence to demonstrate these are always applied and are effective.	Documented and complete processes in place to ensure individuals know how to correct their personal information, and to ensure corrections are made when requested. Processes ensure that the corrected information is provided to relevant third parties. Requests for correction of personal information are recorded, monitored, and reported. Assurance/evidence is obtained to show compliance with the principles on correcting personal information, or there is a plan in place to obtain this assurance/evidence.	Documented and complete policies and processes are in place to: • track correction requests • validate the accuracy and completeness of such data • ensure appropriate justification is documented when data is not updated to relevant third parties. Assurance/evidence is obtained to demonstrate compliance with/effectiveness of these policies and principles and to identify exceptions.	There are documented and complete policies and processes in place to monitor and assess: • timelines and responses to correction requests • justification for not providing information updates to relevant third parties. Updating is automated and self-service where possible and appropriate. Distribution of updated information to third parties is also automated where possible and appropriate. Assurance/evidence is obtained to demonstrate compliance with/effectiveness of these policies and principles and to identify exceptions. All complaints and/or concerns relating to access of information are reviewed and improvement opportunities identified and implemented as a result.
		IPP 8: Accuracy	Informal, undocumented, or inconsistent processes and controls for ensuring the accuracy of personal information.	Some documented procedures to ensure personal information is not used or disclosed without taking reasonable steps to check it is accurate, complete, relevant, up to date, and not misleading, but the agency does not obtain evidence to show these are always applied and are effective.	Documented and complete processes in place to ensure that personal information is not used or disclosed without taking reasonable steps to check that it is accurate, complete, relevant, up to date, and not misleading. 'Reasonable steps' is defined in the context of the agency's operations.	Assurance/evidence is obtained to demonstrate compliance with/effectiveness of these policies and principles and to identify exceptions.	All complaints and/or concerns relating to accuracy of information are reviewed and improvement opportunities identified and implemented as a result.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
		IPPs 9–11: Use and disclosure	Informal, undocumented, or inconsistent processes and controls on using and disclosing personal information.	Some documented procedures to ensure the use and disclosure of personal information to third parties is only for the purposes for which it was collected and for which the individual has provided consent, unless laws or regulations allow otherwise, but the agency does not obtain evidence to show these are always applied and are effective.	Documented and complete processes in place on the use, redaction, and disclosure of personal information, both internally and to third parties. Policies cover: • who takes decisions about disclosures and new uses, and what process is required to ensure any disclosures or new uses comply with the law and are in the interests of the agency • documentation of any disclosures or new uses of information • factors that need to be considered when deciding whether to disclose • integration of use and disclosure policies into the wider privacy strategy.	Assurance/evidence is obtained to demonstrate compliance with/effectiveness of these policies and principles and to identify exceptions.	All complaints and/or concerns relating to access of information are reviewed and improvement opportunities identified and implemented as a result.
		Retention	Informal, undocumented, or inconsistent processes and controls for disposing of and destroying personal information.	Some documented procedures for appropriately disposing and destroying personal information, but the agency does not obtain evidence to show these are always applied and are effective.	Documented and complete processes are in place to ensure the appropriate disposal and destruction of personal information align with the Privacy Act 1993 and the Public Records Act 2005, and any other relevant regulations specific to the agency. Disposal schedule for the various types of personal information has been verified as complete against the agency's personal information inventory. Assurance/evidence is obtained to demonstrate compliance with the principles around retention and to identify exceptions.	Policies and procedures for disposal and destruction of personal information are reviewed regularly, and also reviewed in response to new types of personal information identified on the agency's personal information inventory.	Assurance/evidence on third parties' processes for disposing of and destroying the agency's personal data (eg archiving companies) is obtained. All complaints and/or concerns relating to access of information are reviewed and improvement opportunities identified and implemented as a result.

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	**Developing**	**Defined**	**Embedded**	**Optimised**
9	**Breach and incident management**	**Incident handling and escalation process**	No structured approach to incident management and little documentation or support from privacy specialists.	Staff awareness of the possibility of a privacy breach is limited to inadvertent disclosure to external parties. Existing informal incident response processes, which are managed within business units with limited central oversight.	Documented incident response and escalation procedures in place, of which staff are aware. Agency-wide understanding of what a privacy incident is (including complaints, 'near misses', and breaches). All staff and management know how to respond to an incident; particularly who to inform, how they should be informed, and the timeframe for communication.	Privacy complaints, 'near-misses' and breaches are recorded and root-cause analysis is undertaken to inform subsequent changes and improvements to processes. The agency has a comprehensive and consistent approach to incident management, which covers incidents relating to all of the Information Privacy Principles. A hierarchy of 'trigger points' for escalation to appropriate levels of management exists.	Internal and external privacy environments are monitored for issues affecting the appropriate response to a breach. Improvements to processes are proactively made as a result. Any large-scale incidents are managed in accordance with the agency's crisis management approach. All incidents are subject to a post-incident review to assess the incident response. Any resulting improvements to processes are implemented in a timely manner.
		Breach/incident reporting	Undefined reporting requirements on privacy breaches.	Breaches recorded and reported to management relate mainly to inadvertent disclosure of personal information to third parties (and do not focus on the other IPPs).	An approved process for recording and reporting on personal information breaches and near misses relating to all of the IPPs is in place. Regular reports on breaches, including actions taken to remedy these, are made to executive management.	An approved process for recording and reporting on personal information breaches, near misses, trends, risks, and other relevant information to the appropriate levels of management is in place.	Systematic/systemic analysis is used to inform changes to processes/procedures.