New Zealand Government

User guide for the Privacy Maturity Assessment Framework (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 (2014). *User guide for the Privacy Maturity Assessment Framework (version 1.0)*. 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 *Privacy Maturity Assessment Framework: Elements, attributes, and criteria (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/.

ISBN 978-0-478-40856-0 (online)

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

Contents

1 Purpose of this document

This document is a user guide for the Privacy Maturity Assessment Framework. It outlines the purpose of the framework and explains how it can be applied and used.

Access the Privacy Maturity Assessment Framework in the Privacy Leadership Toolkit on the Public Sector Intranet (available to subscribed public sector agencies). Read this user guide in conjunction with:

- *Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 2.0)* (PDF)
- Privacy Maturity Assessment Tool – an Excel tool for recording ratings and providing visual summaries.

2 Executive summary

The Privacy Maturity Assessment Framework enables agencies to assess and improve their privacy practices.

The framework will help agencies understand their current maturity and capability levels, know how they compare with better practice, and identify what they need to do for continuous improvement. It will also enable agencies to set targets, identify and prioritise key improvements to achieve these targets, and demonstrate improvement in managing privacy.

Any individual, agency, or business, whether in the public or private sector, which holds personal information on an individual is required to comply with the Privacy Principles of the Privacy Act 1993.[1] This framework incorporates these compliance requirements as well as better-practice targets.

The framework consists of nine elements that provide criteria against which an agency can assess their privacy maturity. Maturity is assessed through five possible maturity levels.

Through the framework, agencies can select – against each of the framework's attributes – the maturity levels that best represents them. They can also set their desired target levels indicating where they can improve in the long term.

The Privacy Maturity Assessment Tool can be used to record their current state, short- to medium-term targets, and longer-term goals.

Principles

The principles that underpin the framework are:

a. **simple, pragmatic, and easy to use** – use of the tool can be maximised without significant investment by agencies
b. **consistent assessment across the public sector** – this will enable standards and/or best practice guidelines and the potential for benchmarking practices to be developed in the future
c. **scalable** – is useable by all types of agencies
d. **risk management focused** – agencies can set their targets based on their own privacy risk profile
e. **maturity model** – continuous improvement can be made across the key areas needed to better manage personal information.

[1] Unless the individual, agency, or business is specifically excluded as per s(2)(1)(b) of the Privacy Act 1993.

3 The Privacy Maturity Assessment Framework

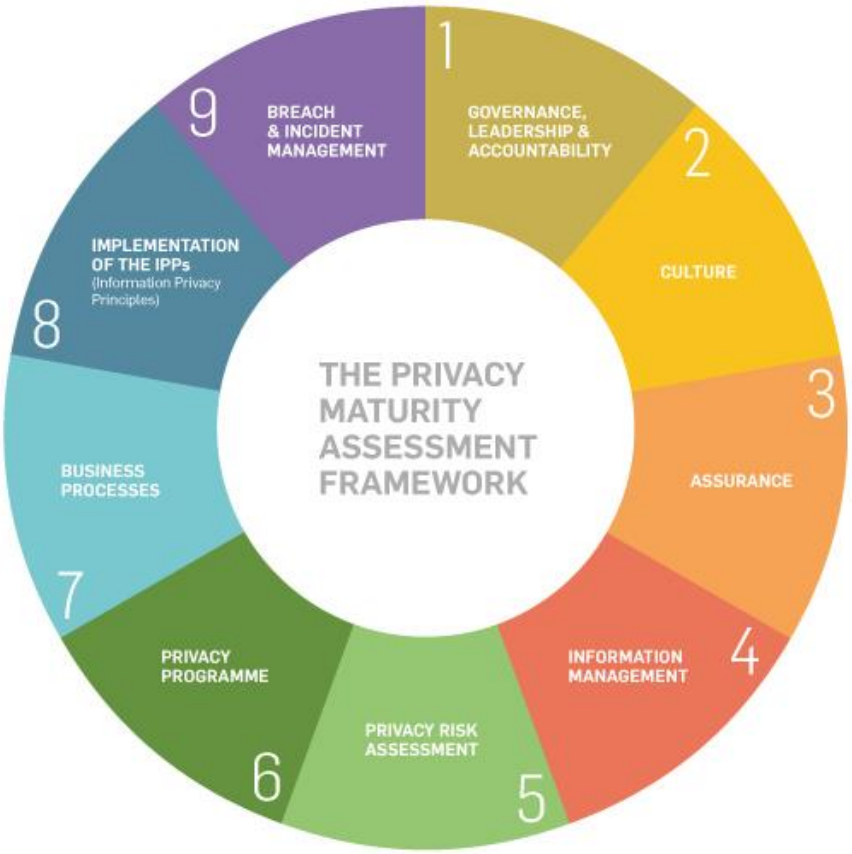
This chapter lists the nine elements of the Privacy Maturity Assessment Framework and the maturity levels used in the framework.

The framework consists of nine elements, which contribute to the overall privacy environment:

1. governance, leadership, and accountability
2. culture
3. assurance
4. information management
5. privacy risk assessment
6. privacy programme
7. business processes
8. implementation of the Information Privacy Principles
9. breach and incident management.

Figure 1

Elements of the Privacy Maturity Assessment Framework



Each element has a number of attributes and criteria against which you can assess your privacy maturity. Maturity is assessed through five possible maturity levels described in table 1.

Table 1

Maturity levels

Maturity level	Description
N/A	Attributes are not applicable or a high priority, based on a mature understanding of organisational risks and risk appetites.
Ad hoc	Unstructured approach where privacy policies, processes, and practices are not sufficiently defined or documented. Privacy management is mostly dependent on initiatives by individuals rather than processes.
Developing	Privacy management is viewed as a compliance exercise and the overall approach is largely reactive with some documented guidelines. There is limited central oversight of the privacy policies, processes, and practices, with siloed approaches within business units.
Defined	Privacy policies, processes, and practices are defined and comprehensive to meet the operating needs of the agency and are consistently implemented throughout. The business has a holistic and proactive approach with widespread awareness of privacy management.
Embedded	Privacy management is embedded into the design and functionality of business processes and systems and is consistent across the agency. Well-defined governance and oversight structures exist.
Optimised	Privacy management is viewed as a strategic initiative with a clear agency culture of continuous improvement. The agency is viewed by stakeholders and the public as a leader in privacy management, introducing innovative initiatives to meet their needs.

Each maturity level builds on the previous level(s) within each attribute; all the criteria specified within one maturity level are to be achieved before moving on to achieving the next level of maturity. However, an agency could decide, based on a mature understanding of organisational risks and risks appetites, that elements of a maturity level are not applicable or a high priority. The tool does not enable ‘Graded’ maturity ratings to be assigned, but evidence of decisions and ratings should be documented. The attributes are not mutually exclusive and the evidence gathered to support your rating for one attribute may also support other attributes. See Appendix 3 for examples of what an agency with immature or mature attributes might look like.

4 Applying the Privacy Maturity Assessment Framework

This chapter provides general guidance on how to use and apply the framework for assessing privacy capability and maturity. It also explains what you should consider when identifying the resources needed and when gathering evidence to support the assessment.

As the Framework is designed to assess the elements of privacy management in place within an agency, certain basic aspects of privacy management are required in order to enable assessment. If an agency does not have any form of privacy or data management programme, strategy or approach in place, there is little value in undertaking an assessment. In this instance, the Framework may instead be used as a guide for developing an approach to privacy.

Through the framework, you can select the maturity level that best represents your agency's current level of maturity for each of the attributes. You can also set your desired target level and long-term better-practice targets.

Individual elements or attributes of the Framework can also be used/assessed (and others left out) if an agency decides to prioritise certain aspects, address specific risk, or where certain elements or attributes are considered to not be applicable.

The scope and approach to assessing privacy maturity will differ across agencies. This is due to the inherent maturity-level differences (in relation to both privacy and assurance/assessment experience), agency size and type, and the volume and types of personal information an agency holds. These differences will also inform the privacy risk assessment required for setting appropriate targets. The information in this chapter is therefore intended as a general guide only, for use by all agencies despite their differences.

Some of the possible approaches for evidence collection are shown below. This is not an exhaustive list and is intended for guidance only:

Approach / process	Advantages of approach	Disadvantages of approach
Informal self-assessment a. Conversations with key staff and management, and collection of evidence as identified during the process	• Can be used to explain privacy and the "bigger picture", and raise awareness • Able to be conducted with limited resources (although can still be time consuming)	• Less structured approach may lessen confidence in the results • May not be comprehensive in terms of coverage of agency's scope and operations • Unlikely to be appropriate for an agency with significant privacy risk.
b. Workshops with a range of staff and management - Discussion-based collection of information	• Can cover all of the agency's operations/functions, and levels of management and staff • Staff/management	• Lack of awareness of privacy work results in lower ratings even if work is underway or has been completed

	awareness of documentation or process is evidence in itself and an opportunity for education • Can be used to explain privacy and the "bigger picture", and raise awareness • If externally-facilitated, may result in more open feedback	• Depends heavily on staff motivation to attend workshops and participate in discussion • Involvement of large number of staff and managers required • Does not focus on evidence (however may be combined with other approaches to give an overall picture)

Structured project self-assessment
 	
- Project team established, including people with expertise in personal information management
- Process for gathering information includes:
  ○ surveys
  ○ review of documentation
  ○ workshops/fora with staff, management and the governing body(s) across the organisation
  ○ conversations with key individuals
	• Wide involvement and viewpoints from across the agency, including the governance layer
	• Can be used to explain privacy and the "bigger picture", and raise awareness
	• Can cover all of the agency's operations/functions, and levels of management and staff
	• Evidence-based
	• Work can be re-performed for reassessment against the baseline
	• Provides a structured approach
		• Requires participants to attend workshops and participate in discussion
		• Involvement of large number of people required (with associated time and cost implications)

Independent assurance / assessment (e.g Internal audit) methodology: - Evidence collection and assessment - Interviews with key staff and management - Evaluation of compliance with the framework and internal policies and procedures - Formal reporting with recommendations	• Evidence-based • Work can be re-performed for reassessment against the baseline • Provides a structured approach and a report with recommendations, which may be appropriate for improvement for agencies with higher privacy risk • May provide a higher level of visibility with the executive.	• May be expensive • May be seen as a compliance exercise rather than an opportunity to improve or to educate • Process may not capture the required information or level of detail to understand the changes / improvements needed • Care needed when drawing up terms of reference.

The above approaches may be used whether a self- or independent assessment is undertaken. An independent assessment may utilise internal capabilities or bring in

external resources. If a self-assessment is used then it is recommended that a periodic (regular) independent review of the results is obtained.

Assessing against the framework, no matter which approach is used, has been shown to provide value in itself; particularly in terms of raising the profile of privacy and demonstrating that privacy considerations are much broader than focusing on breaches.

The following steps should be considered when assessing your agency's privacy maturity.

1. Determine your current state for each attribute in the framework.

   a. Collect evidence and identify your current privacy culture, documentation, practices, and knowledge. The framework contains details on what is expected for each attribute, which you can use to identify the evidence you need to research, identify, and gather. Evidence should be collected from a range of people across the agency's operations and across different levels of staff and management in order to give a comprehensive picture. Engagement with senior level management and members of the governance group(s) is critical; as well as incorporating their knowledge in the assessment stage and obtaining their agreement as to the appropriate targets, this provides an opportunity to improve the visibility of privacy management.

   b. Document the evidence under the 'Comments' section of the Privacy Maturity Assessment Tool. [2]

   c. Select the level of maturity (ad hoc, developing, defined, embedded, or optimised) that best reflects your current state in relation to each attribute, based on the evidence gathered.

   d. Record your current state and the evidence to support this. You may use the Privacy Maturity Assessment Tool for this purpose.

2. Determine your targets for improvement.

   a. Once you have identified your current state, identify your desired targets and when you intend to achieve these (eg. 18 months). This period will differ between agencies and should take into account what can realistically be achieved.

   b. It is important that you choose your target levels based on the context of the personal information you hold and your risk-tolerance levels. You will need to:

      i. identify the volume and types of personal information held

      ii. assess the risks specific to each attribute through an overall risk assessment[3]

      iii. define your agency's tolerance for privacy risks.

      Due to the nature of the personal information held, the results of a comprehensive privacy risk assessment and the level of tolerance for individual privacy risks, agencies may set different target maturity levels. These are likely to be different even between similar agencies.

   c. The targets should be approved and owned by executive management or the governance board and/or committee(s).

---

[2] The Privacy Maturity Assessment Tool is an Excel instrument used to record the ratings and provide a pictorial representation of the current state assessment against an agency's targets for improvement. See appendix 4 for guidance on how to use the tool.

[3] For guidance on undertaking a formal risk assessment, see ISO31000:2009

3. Determine the better-practice targets you would like to achieve in the long term:

   a. A target rating of 'optimised' is not necessarily relevant to all agencies and all attributes. The risk assessment, including the risk tolerance levels, should inform the level you aspire to (eg higher risk and lower tolerance means you should aim for a higher level of maturity, for example embedded or optimised).

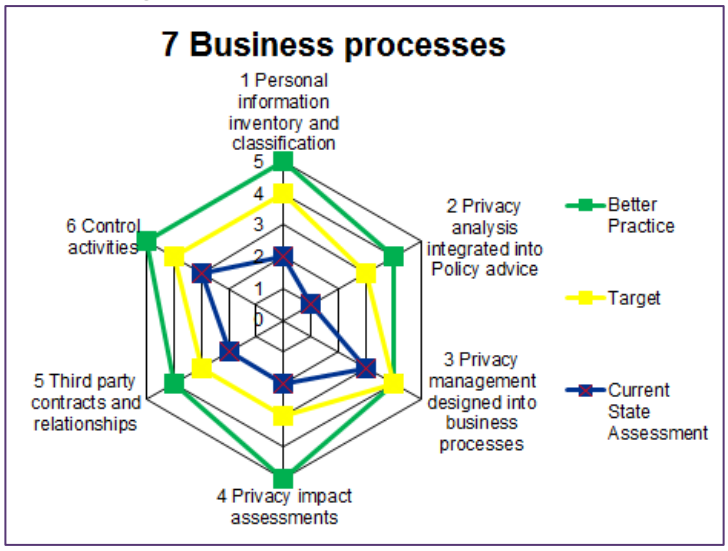
   b. The targets should be approved by executive management or the governance board and/or committee(s).

The Privacy Maturity Assessment Tool also generates a summary 'spider' diagram for each element. This diagram shows your assessment for each of the attributes of an element against your target and better-practice ratings.

See figure 2 for an example of a spider diagram for the business processes element.

Figure 2

Spider diagram example – business processes



The tool also generates an overall summary 'spider' diagram for the framework that shows an agency's maturity for each of the elements against the overall target and better-practice ratings (see figure 3).

4. Report results

a. The results of the current state assessment and the targets determined should be reported in a manner that is relevant and sufficient for the audience. Different audiences will require different types of reporting. Examples include:

   i. Governance layer
   The report to the governing body is intended to inform, and obtain support. Results are likely to be summarised and focus on the overall results (e.g. the spider diagram showing the overall ratings (see Figure 3) is likely to be of more interest to this audience than detail on every attribute.

   Other means of presenting summarised results may include bar graphs or pictorial representations.

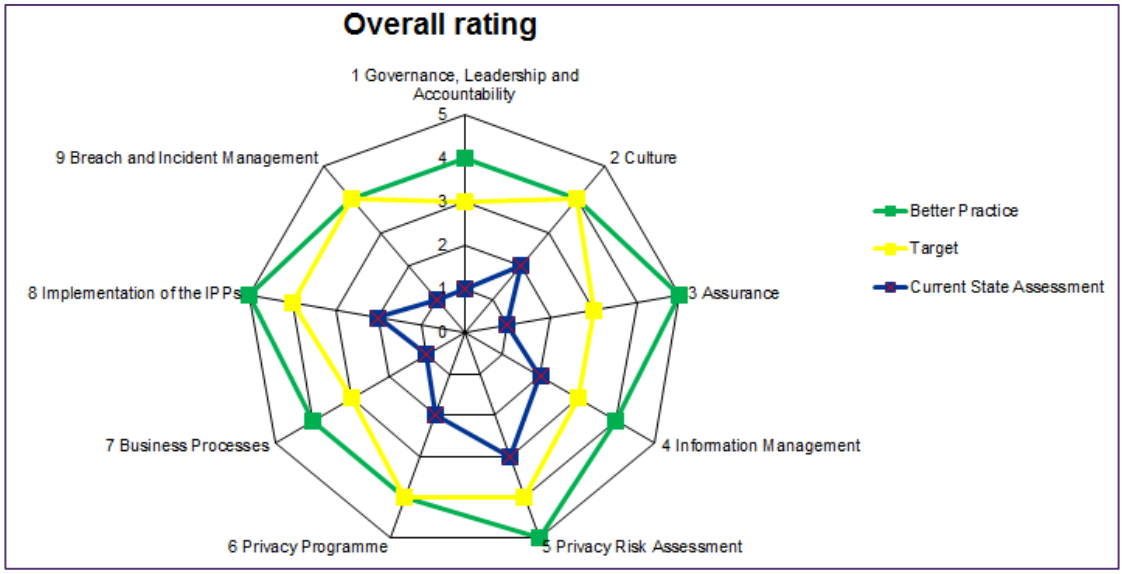
ii. Privacy Officer / assessment team

This audience will require detailed results for each element and attribute that was assessed during the process, including the spider diagrams for each (see Figure 2 for an example). This may be presented in tabular form, with current state and target ratings presented for each attribute, along with observations/evidence/recommendations for improvement for each attribute where there is a gap between the current state and target ratings.

iii. Other staff

Participants in the assessment and other staff are also likely to be interested in the results. This could include summary results as well as reporting that is focused on results at the attribute layer. This could be presented by providing the spider diagrams for each element.

Figure 3
***Spider diagram example* – overall rating**



4.1 Resourcing

The time and resources an agency needs to complete their self-assessment will vary, depending on the size and complexity of the agency, knowledge level of the assessor, and how readily accessible the evidence is.

When you have completed a self-assessment of your current state, further time and resources will be needed for reporting this to the executive management and governance board and/or committee(s), and determining the appropriate better-practice targets for your agency.

Assessment

An appropriate person or team should be responsible for undertaking a privacy maturity assessment. We recommend that the team have a mix of the following skills and experience:

- experience in undertaking audits, assurance activities, evaluations, or equivalent
- specialist knowledge of good practice privacy management
- is not the agency's Privacy Officer (as the effectiveness of the role of the Privacy Officer is assessed within the framework).

Examples of appropriate team members who may collaborate to complete the assessment may include:

- staff from Risk and/or Assurance teams
- staff from a Business Improvement team
- privacy professional from another agency
- independent assurance provider.

We also recommended that agencies consider participating in peer assessments with other agencies.

A self-assessment is likely to consist of:

- interviews with management and staff, both at the national office and other sites
- documentation gathering, review, and analysis
- site visits
- surveys to understand roles, privacy risks, and aspects of organisational and privacy culture.

At a small or medium-sized agency, a dedicated review where evidence is readily accessible is likely to take between one and three weeks. However, a review will usually take a longer time (between six and eight weeks, or more, accounting for elapsed time) if a survey is used and/or sites are visited.

Improving capability

Each agency will prioritise the elements and attributes differently.

The first step to improving privacy capability is to know the volume and types of personal information your agency collects, uses, and discloses. This should then be recorded and kept as your 'personal information inventory'. Creating this inventory is a key step and may not be straightforward, particularly for large or complex agencies that hold significant volumes of personal data.

The next step is to undertake a risk assessment, which will be used to define your privacy strategy. The risk assessment is also the best time to set your target maturity levels.

You should be aware that capability improvement (demonstrated by an increase in the ratings within the framework) may take some time and resources to realise, so be realistic in your expectations.

The results of the self-assessment, and the gaps between the current state assessment and the targets, may be used to develop a work programme that focuses on closing the identified gaps.

It could take between 6 and 12 months for an agency to move up one level of maturity. Movement depends on a number of factors, including the size and current maturity of the agency, the volume and types of personal information held, and the resources available for privacy maturity improvement.

4.2 Evidence

The purpose of the framework is to provide a self-assessment tool for improving privacy capability and maturity. However, when determining the amount of evidence required, you should consider that there could be external as well as internal interest in your results. Your assessments and evidence should therefore be able to satisfy any future expectations of external assurance agencies.

The Tool includes a 'Comments' field for each Attribute. As noted earlier, 'graded' ratings cannot be assigned; however the Comments field may be used to reflect progress made or movement within the ratings and capture evidence of these.

The way criteria in each attribute is applied and the focus areas of agencies when assessing against the framework means that the detail and type of evidence collected will differ between agencies. This is why the assessments should be undertaken by people with experience in undertaking audits, assurance activities, and evaluations.

Recording and keeping your evidence accessible is important because:

- it increases confidence in your results
- it can be presented to interested parties to support the validity of your assessment
- you will be able to easily access and use it when re-assessing against the framework to identify improvements in maturity levels.

At a minimum, the person undertaking the assessment should record what was found, where it was found, and how it was verified.

Appendix 1: Framework development

Statistics NZ developed the framework in 2013 as part of the Privacy Leadership Programme under the Information Privacy and Security Governance Group. KPMG was contracted to work on the framework development. A number of government agencies also contributed their expertise.

The steering committee overseeing the development included representatives from the Office of the Privacy Commissioner, Department of Internal Affairs, Inland Revenue, Ministry of Justice, Ministry of Social Development, and Statistics NZ.

The development process also included several workshops that included participants from Accident Compensation Corporation, Ministry of Business, Innovation and Employment, Department of Corrections, Earthquake Commission, Inland Revenue, Ministry of Justice, Tertiary Education Commission, and Statistics NZ.

Initial workshops were also held with the Privacy Working Group and Privacy Leadership Forums, set up under the Privacy Leadership Programme. These workshops included representatives from:

Accident Compensation Corporation
Canterbury Earthquake Recovery Authority
Department of Corrections
Department of Internal Affairs
Earthquake Commission
Inland Revenue
Ministry of Business Innovation and Employment
Ministry of Education
Ministry of Health
Ministry of Justice
Ministry of Social Development
New Zealand Police
New Zealand Qualifications Authority
Office of the Privacy Commissioner
State Services Commission
Statistics New Zealand
Tertiary Education Commission.

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. With the establishment of the Government Chief Privacy Officer in 2014, responsibility for the framework was transferred to the Department of Internal Affairs.

Appendix 2: Examples of Privacy Immaturity and Maturity

Element	Immature agency (examples only)	Mature agency (examples only)
Governance, Leadership & Accountability	• Members of the leadership team do not demonstrate a privacy focus, or receive or provide information and resourcing for privacy unless a high profile issue is identified • No Privacy Officer or documented privacy approach	• The Privacy Officer has the tools to proactively monitor and improve privacy management • The agency's approach to privacy is documented, well known and supported at all levels
Culture	• Lack of guidance on what good privacy management, breach identification and organisational values are	• Leadership 'model' good privacy behaviour • All levels of staff and management see privacy as important
Assurance	• Limited or no assurance over privacy processes and controls	• Three lines of assurance model for privacy is embedded as business as usual • Processes change as a result of opportunities identified through assurance
Information Management	• Principles and implementation of appropriate information management aren't known across the organisation • Strategy and business processes aren't documented and known, nor do they explicitly include privacy considerations	• Privacy is included as business as usual within the information management structure, strategy and business processes. This is risk-based and integrated into the overall business strategy • Information is considered an asset and treated as such
Privacy Risk Assessment	• Privacy risk is treated separately from business risk, or is not explicitly considered and mitigated	• Privacy is included as business as usual in the overall enterprise risk framework • Risk assessment is proactive and effective. Risks are monitored, analysed and reported

Privacy Programme	• There is unclear, or no, direction on how to best approach privacy considerations, including a lack of training for staff and contractors • Lack of effective and up-to-date privacy policies and procedures, and communication with staff on privacy	• A comprehensive privacy programme is in place; which is risk-based, covers the entire organisation, is reflective of changes to the privacy environment, and considers privacy a core competency • Policies and procedures are proactively updated as requirements change • Training on privacy includes contractors as well as staff. Understanding is demonstrated before access is given to personal data • There is clear, ongoing communication across the organisation regarding privacy management and effectiveness
Business Processes	• Lack of formal processes and controls for mitigating privacy risk • Third parties who have access to personal data are not included in the agency's privacy programme	• Formal processes are undertaken to ensure the agency knows what personal data it holds, what this data consists of including its sensitivity, how much there is and what it is used for. This is documented, regularly assessed, and used to design business processes • Third parties are expected to treat personal data as the agency does, and assurance over this is required • Controls are in place to ensure privacy risk is mitigated and issues are identified quickly. Control effectiveness is reviewed. Continuous monitoring is in place
Implementation of the Information Privacy Principles (IPPs)	• No formal, documented or consistent processes and controls in place that cover the IPPs, or a lack of assurance on the effectiveness of these	• Documented and complete policies and procedures are in place that cover each of the IPPs • Assurance/evidence is obtained to demonstrate compliance with and effectiveness of these policies and principles and to identify exceptions • Complaints and concerns are reviewed and improvement opportunities are implemented as a result
Breach & Incident Management	• No planning for when a breach may occur, and staff are not aware of what to do.	• Complaints, 'near misses' and breaches are included in analysis that informs change • Breach and incident responses are activated when any of the Information Privacy Principles are not complied with (i.e. not solely when personal information is inadvertently released).

Appendix 3: Glossary

The following terms are used in the framework as defined below.

Accountability	Being liable or answerable for a process or outcome.
Agency	New Zealand public sector organisation that falls under the jurisdiction of the Privacy Act 1993, as described in s(2)(1).
Assurance model	The framework used to provide assurance (verified information to enable decision-making) for an agency (see three lines of assurance).
Control activities	The measures used to help ensure that management directives are carried out and that risks are addressed. They take many forms, including policies and procedures, approvals, verifications, performance reviews, and security measures.
Data breach	An instance where personal data is inappropriately made available.
Governance	Decisions that define expectations, grant power, or verify performance. It consists of either a separate process or part of decision-making or leadership processes.
Information Privacy Principles (IPPs)	The Principles are at the core of the Privacy Act. They set out how agencies may collect, store, use, and disclose personal information.
Leadership	Senior management or governing body.
Privacy policy	Documented requirements for managing or dealing with privacy-related processes or risks.
Privacy risk	The risk of not adequately managing privacy, resulting from inadequate or failed internal processes, people and systems, external events, or poor strategic business decisions.
Privacy risk appetite/tolerance	The level of risk that an agency is prepared to accept, before action is deemed necessary to reduce it. It represents a balance between the potential benefits of change and the threats that change inevitably bring.
Three lines of assurance	A formal, planned programme of assurance covering the first line (business operations), second line (oversight functions), and the third line of assurance (independent assurance).

Risk management function	The part of the agency responsible for driving and administering risk management processes.
Personal information	Any information about an individual (a living natural person) as long as that individual can be identified.
Privacy breach	The result of unauthorised access to or collection, use or disclosure of, personal information. In this context, 'unauthorised' means in contravention of the Privacy Act 1993.
Privacy complaint	A formal complaint by an individual relating to non-compliance, or perceived non-compliance, with the Information Privacy Principles or other requirements.
Privacy incident	An instance where personal data has not been made available to inappropriate person(s) but there has been the potential for this to occur.
Privacy management function	The part of the agency responsible for driving and administering privacy management.
Privacy programme	Planned and defined actions to be taken across the agency in respect of privacy.

Appendix 4: Privacy Maturity Assessment Tool – user guide

Purpose

The Privacy Assessment Tool ('the tool') is used to record and summarise an agency's self-assessed maturity levels using the Privacy Maturity Assessment Framework.

Minimum requirements

The tool is an Excel instrument. To use the tool you will need to have at least Microsoft Office Excel 97-2003.

Structure of the tool

There are nine sections that make up the overall assessment tool: one section for each of the elements covered in the Privacy Maturity Assessment Framework:

1. governance, leadership and accountability
2. culture,
3. assurance,
4. information management,
5. privacy risk assessment,
6. privacy programme,
7. business processes,
8. implementation of the IPPs,
9. breach and incident management.

The tool can be navigated using the main menu.

Each section consists of:

- the attributes that together make up each element
- maturity level ratings for each attribute, representing the agency's privacy management self-assessment and targets:
    - current state assessment – the self-assessed level of maturity of the agency's current performance in relation to each attribute
    - target – the level of maturity the agency aims to achieve within the next 18 months
    - better practice rating – represents the maturity-level target to which the agency aspires to achieve in the longer term, based on an agency-specific risk assessment.
- definitions of what current, target, and better practice may consist of (ie how they might be demonstrated by the agency) are included in the 'ratings definitions' fields. There are definitions of maturity level ratings for each of the attributes within each of the elements
- a 'Comments' field, which may be used to record the evidence obtained.

The maturity level ratings that may be selected for each of the attributes are:

Maturity level	Description
N/A	Attributes are not applicable or a high priority, based on a mature understanding of organisational risks and risk appetites.
Ad hoc	Unstructured approach where privacy policies, processes, and practices are not sufficiently defined or documented. Privacy management is mostly dependent on initiatives by individuals rather than processes.
Developing	Privacy management is viewed as a compliance exercise and the overall approach is largely reactive with some documented guidelines. There is limited central oversight of the privacy policies, processes, and practices with siloed approaches within business units.
Defined	Privacy policies, processes, and practices are defined and comprehensive to meet the operating needs of the organisation and are consistently implemented throughout. The business has a holistic and proactive approach with widespread awareness of privacy management.
Embedded	Privacy management is embedded into the design and functionality of business processes and systems and is consistent across the organisation. Well-defined governance and oversight structures exist.
Optimised	Privacy management is viewed as a strategic initiative with a clear organisational culture of continual improvement. The organisation is viewed by stakeholders and the public as a leader in privacy management, introducing innovative initiatives to meet their needs.

The tool produces pictorial representations (spider diagrams) of the self-assessment and target ratings specific to the organisation.

How to use the tool

Details on how to select a rating to reflect the agency's current, future, and aspirational targets is included in chapter 4, Applying the Privacy Maturity Assessment Framework.

To enter the ratings in the tool and generate the spider diagrams:

1. Open the file: PrivacyAssessmentTool.xls.
2. Select an element tab, depending on which element is to be assessed.
3. For each attribute within the element tab, click on the drop-down box in each of the current state assessment, target, and better practice columns and select the relevant maturity level (ad hoc, developing, defined, embedded, or optimised).
4. As the current state assessment, target, and better practice ratings are completed in the tool, the spider diagram will update at the bottom of each page; giving a pictorial representation of the ratings.
5. In addition to a spider diagram representing each of the elements, an overall depiction of all of the elements combined (ie the overall maturity levels across the Privacy Maturity Assessment Framework) is shown in a spider diagram in the 'overall rating' tab.

You can record any evidence or your notes on how you undertook the assessment in the 'Comments' field of the tool.

Appendix 5: Further reading

The following resources on privacy may help you when undertaking a privacy maturity self-assessment.

American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (2011). AICPA/CICA privacy maturity model. Available from www.cica.ca.

American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (2009). Records management: Integrating privacy using generally accepted privacy principles. Available from www.aicpa.org.

Information and Privacy Commissioner Ontario, Canada (2010). Privacy risk management. Available from www.ipc.on.ca.

Institute of Internal Auditors (2006). Managing and auditing privacy risks. Available from https://na.theiia.org.

International Organization for Standardization (2009). ISO 31000: 2009 Risk management – principles and guidelines. Available from www.iso.org.

Office of the Information and Privacy Commissioner of Alberta (nd). Getting accountability right with a privacy management program. Available from www.privacyassociation.org.

Office of the Privacy Commissioner (2007). Privacy impact assessment handbook. Available from www.privacy.org.nz.

Office of the Privacy Commissioner (updated 2008). Privacy breach guidelines. Available from www.privacy.org.nz.