Government Chief Privacy Officer

**Privacy Maturity**

**Self-Assessment Report**

**June 2024**

**[agency name here]**

## Reporting period for self-assessment

The reporting period for PMAF is the financial year (that is, **1 July to 30 June**).

Obviously, you will need time to get the report signed off before the submission deadline of 30 June, and may be unable to state exactly what your position will be at that time. Simply do your best to make the information as up to date as possible for us.

## Completing a self-assessment

There are two documents that make up the PMAF self-assessment:

## The Excel Spreadsheet for agency maturity ratings; and

## This Word template for maturity assessment analysis.

This Word template has separate tables to describe each element of privacy maturity and the criteria that give more detail for each element.

* In the right-hand column where the template says “Type rating here”, replace that highlighted text with one of these three values: **Informal, Foundational** or **Managed**
* Choose whichever of those values best reflects your agency’s maturity for that specific criterion. There is a direct link to our PMAF guidance under each of the four main headers to help you decide which word is most accurate.
* Put the same values for each criterion into the accompanying Excel Spreadsheet. This will calculate your agency’s overall privacy maturity.
* Wherever possible, add detailed comments to all four comment fields: Context, Achievement, Future Focus, and Challenges. Please follow our advice below about writing effective comments.

## What to send to GCPO

Please send both your completed Excel and Word files (or Word files as PDFs) to [GCPO@dia.govt.nz](mailto:GCPO@dia.govt.nz) by **30 June 2024.**

It is important to ensure that the Chief Executive signs this document. If this is not possible by 30 June, please submit your unsigned copy by the deadline and then send us a scan of the signature page as soon as possible afterwards.

## Writing effective comments

Detailed comments are essential to help us understand your agency and its privacy environment. Comments also let us develop our system insights, such as identifying where there are gaps to fill, or experience that can be shared.

Effective comments:

* relate to the specific aspect of privacy maturity that the document is asking about
* show evidence of why the selected level was chosen (linked to the description for that maturity level)
* are clear, concise and to the point
* provide specific information about the GCPO’s focus areas. For 2024, these are:

1. Reducing the number of areas where agencies are at Informal maturity (include as general comment)
2. **Core Expectation 5.1:** Identifying Māori privacy interests
3. **Leadership 3.1:** Privacy and assurance
4. **Core Expectation 1.3:** Being transparent

### Where to go for more help

For more information about PMAF or about completing a report, please email us at [GCPO@dia.govt.nz](mailto:GCPO@dia.govt.nz)

# Chief Executive Summary Report

|  |  |
| --- | --- |
| **To** | Katrine Evans, Government Chief Privacy Officer |
| **From** | [Insert Chief Executive name and title] |
| **Date** | [insert date] |

Attached is my report outlining progress on building privacy capability within my agency and meeting the core expectations set by the Government Chief Privacy Officer.

Below I have provided further comments about the development of privacy maturity in our agency and the completion of this assessment.

|  |
| --- |
| I would like to provide the following comments: |
|  |

### Validation Statement

I have assurance from my agency that the scores and comments below are true and correct.

Signature:

Name: [insert Chief Executive name and title here]

Date: \_\_\_\_\_\_ / \_\_\_\_\_\_ / \_\_\_\_\_\_\_\_

### Does your agency collect any of the following types of information?

Please indicate with a tick ( **✓** ) in these columns if your agency collects any of the following types of personal information. Please tick both if direct and indirect collection happens.

* **Direct collection:** received from the individual or their authorised representative.
* **Indirect collection:** received from a third party such as another government agency under a MoU or AISA, non-government organisations, service providers, etc.

|  |  |  |
| --- | --- | --- |
| Type of Information  Brief description of examples of the type of information defined; not a definitive list | Direct collection | Indirect collection |
| Biometric  Information about an individual’s physical or behavioural features: fingerprints, face, voice, gait, etc. |  |  |
| Children  Information about children and young people’s including health, education, well-being, consent, etc. |  |  |
| Criminal and justice  Information about an individual’s offending, charges, sentencing reports, probation, etc. |  |  |
| Employment  Information about individual’s employment such as Human Resources, payroll, work history, etc. |  |  |
| Family and community  Information about an individual’s involvement with social organisations, family relationships, etc. |  |  |
| Financial  Information about individual’s finances separate to payroll, such as tax, fraud, AML compliance, etc. |  |  |
| Health  Information about individual’s health, illnesses, and relating to the Health Information Privacy Code |  |  |
| Intelligence and security  Information such as operational intelligence and the protection of New Zealand’s national security |  |  |
| Research and statistics  Including demographic, aggregated, deidentified, and authorised use of the StatsNZ IDI for research |  |  |
| Unique Identifiers  Including those issued by your agency and collected from others |  |  |

### Would you like to provide over-arching comments? (optional)

Explain in the box below any comments that provide over-arching qualifiers and comments that apply to all or multiple criteria and provide context for your specific business.

This may be useful for agencies who only collect HR personal information, agencies with regulatory functions or powers for mandatory collection of personal information, and agencies with a very wide range of responsibilities and functions.

|  |
| --- |
| Over-arching content comments |
|  |

# Core Expectations

[Core expectation guidance](https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-maturity-assessment-framework-pmaf-and-self-assessments/complete-a-self-assessment/core-expectations/)

|  |  |  |  |
| --- | --- | --- | --- |
| Core Expectation 1: Take a people-centred approach to privacy that is respectful of those the information is about and provides the public with effective services. | | | |
| **CE1.1** | **Having a people-centred privacy programme** | **Informal:** Privacy policies and practices are compliance-centric and risk-centric with limited focus on the impact of decisions about use of personal information on the people that the information is about. | Type rating here |
| **Foundational:** Privacy policies and practices include recommendations to consider the views of the people that the information is about. The privacy programme has no specific focus on instilling a people-centred perspective. |
| **Managed:** Privacy policies and practices are appropriately aligned with DPUP’s Principles and Guidelines. The privacy programme focuses on change initiatives to embed a people-centred approach. |
| **CE1.2** | **Connecting with service users** | **Informal:** Individual initiatives infrequently connect with service users to test new ideas with them about collection or use of their personal information. | Type rating here |
| **Foundational:** Individual initiatives connect with service users or their representatives to include their views in decision-making processes about collection and use of their personal information. There is little guidance for initiatives about when and how to go about it. |
| **Managed:** There are established processes and easy-to-use methods for connecting with service users or their representatives, when appropriate, to include their views in decision-making processes about collection and use of their personal information. |
| **CE1.3** | **Being transparent** | **Informal:** Transparency is limited to general clauses in consent forms or privacy notices or statements used at the start of the relationship with service users.  The approach to enabling people to access their information and request correction is ad hoc or reactive. | Type rating here |
| **Foundational:** Individual initiatives focus on transparency about why and how people’s information is collected, used or shared, and what choices they have.  Information about how people can access and request correction of their information is available but is not easy for service users to understand or execute. |
| **Managed:** The agency is transparent about:   * what kinds of personal information it collects and uses * why and how it’s used * choices people may have and how to access and request correction to their personal information.   This information is presented in easy-to-understand ways. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Core Expectation 2: Build and maintain a privacy culture that embodies the public service values of being impartial, accountable, trustworthy, respectful and responsive. | | | |
| **CE2.1** | **Creating a privacy culture** | **Informal:** Leadership has little involvement in the development of a privacy culture. | Type rating here |
| **Foundational:** Leadership recognises the importance of building a privacy culture and focuses on specific areas of the agency or individual initiatives. |
| **Managed:** Leadership delivers consistent and positive messages about how privacy is everyone’s responsibility and how privacy is an enabler of public trust and quality service delivery.  Privacy culture is periodically assessed, possibly as part of a broader organisational culture survey. |
| **CE2.2** | **Communicating privacy values and aspirations** | **Informal:** Communication from senior leadership and privacy leaders is ad hoc or reactive and focuses on specific events and incidents. | Type rating here |
| **Foundational:** Senior leadership and privacy leaders communicate the agency’s privacy values and aspirations as part of specific initiatives and/or work programmes. |
| **Managed:** Senior leadership and privacy leaders communicate the agency’s clearly defined privacy values and aspirations in relevant terms throughout the agency on a schedule that is proportionate to the agency’s needs. |
| **CE2.3** | **Developing privacy awareness** | **Informal:** Privacy awareness is ad hoc or reactive to specific events and incidents. | Type rating here |
| **Foundational:** Privacy awareness is limited and is seen as the responsibility of a few managers and specialists. |
| **Managed:** Privacy awareness clearly communicates the agency’s values, expectations and behaviours to staff and contractors. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Core Expectation 3: Build and maintain privacy capability so that people have the knowledge and skills they need to contribute to good privacy practice. | | | |
| **CE3.1** | **Conducting privacy training** | **Informal:** Privacy training for staff and contractors is conducted on an ad hoc basis. | Type rating here |
| **Foundational:** At induction, staff, and sometimes contractors, receive privacy training on the agency’s privacy values, policies, practices and risks. |
| **Managed:** At induction and then on a regular basis, staff and contractors receive privacy training on the agency’s privacy values, policies, practices and risks that is relevant to their roles and supports them to be effective and trusted custodians of personal information. |
| **CE3.2** | **Monitoring and updating privacy training** | **Informal:** Updates to privacy training content is ad hoc. | Type rating here |
| **Foundational:** Privacy training content is updated periodically. |
| **Managed:** Privacy training needs are monitored and training content is reassessed to ensure that it remains fit for purpose. |
| **CE3.3** | **Providing additional privacy training** | **Informal:** There is little or no additional training for staff and contractors before they are given access to certain classes of personal information (for example, health information) that may fall under a Privacy Code and/or may require additional privacy knowledge to manage properly. | Type rating here |
| **Foundational:** Staff may have additional training before they are given access to certain classes of personal information (for example, health information) that may fall under a Privacy Code and/or may require additional privacy knowledge to manage properly. Contractors generally do not have additional training. |
| **Managed:** Staff and contractors know how to access appropriate advice that they should understand before they are given access to certain classes of personal information (for example, health information) that may fall under a Privacy Code and/or may require additional privacy knowledge to manage properly. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Core Expectation 4: Establish a sense of collective accountability in which managers and staff understand their duty to ensure that personal information is collected and used appropriately. | | | |
| **CE4.1** | **Implementing privacy practices** | **Informal:** Adoption of privacy policies and practices by functional areas that collect or make use of personal information (for example, procurement, service design, contracting and funding, analysis and research, and so on) is ad hoc, and tends to rely on the privacy officer or team involving themselves directly. | Type rating here |
| **Foundational:** Some functional areas that collect or make use of personal information (for example, procurement, service design, contracting and funding, analysis and research, and so on) may reference, or integrate with, privacy policies and practices. |
| **Managed:** Functional areas that collect or make use of people’s personal information (for example, procurement, service design, contracting and funding, analysis and research, and so on) include recognised good practice advice (for example, DPUP) in their core processes. |
| **CE4.2** | **Linking privacy to organisational values** | **Informal:** There is no link between organisational value frameworks, such as mission statements, and the importance of public trust in the collection and use of personal information. | Type rating here |
| **Foundational:** Organisational value frameworks, such as mission statements, include a focus on public trust, but the connection with respectful and transparent practice in the collection and use of personal information is not clear. |
| **Managed:** Organisational value frameworks, such as mission statements, draw a direct line between delivering quality service and exercising a collective focus on respectful and transparent practices in the collection and use of personal information. |
| **CE4.3** | **Including privacy in employment** | **Informal:** There is no clear link made between privacy capability and its role in developing and retaining public trust (for example, letters of employment and job descriptions do not refer to privacy obligations and responsibilities). | Type rating here |
| **Foundational:** There may be a link made between privacy capability and its role in developing and retaining public trust (for example, some letters of employment and job descriptions refer to privacy obligations and responsibilities). |
| **Managed:** There is an agency-wide approach to making the link between privacy capability and its role in developing and retaining public trust (for example, letters of employment and job descriptions refer to privacy obligations and responsibilities). |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Core Expectation 5: Be a capable Treaty partner by supporting the Crown to fulfil its stewardship responsibility and strengthen Crown’s relationships with Māori. | | | |
| **CE5.1** | **Identifying Māori privacy interests** | **Informal:** There is little awareness of the need to identify Māori interests when designing or updating a service or process that involves the collection, use or sharing of personal information. | Type rating here |
| **Foundational:** When designing or updating a service or process that involves the collection, use or sharing of personal information, individual initiatives develop their own practices to identify Māori interests. |
| **Managed:** When designing or updating a service or process that involves the collection, use or sharing of personal information, the agency has policies and practices that can identify relevant Māori interests. |
| **CE5.2** | **Partnering with Māori** | **Informal:** The agency’s identification of and response to Māori privacy interests is ad hoc or reactive. | Type rating here |
| **Foundational:** When Māori privacy interests have been identified, individual initiatives define their own approach for understanding and responding to those interests. |
| **Managed:** When Māori privacy interests have been identified a partnership approach is used and provides for personal information to be interpreted with reference to Māori priorities, values and worldviews. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

# Leadership

[Leadership guidance](https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-maturity-assessment-framework-pmaf-and-self-assessments/complete-a-self-assessment/leadership/)

|  |  |  |  |
| --- | --- | --- | --- |
| Leadership 1: Effective oversight for privacy practice through effective governance. | | | |
| **L1.1** | **Privacy reporting** | **Informal:** The senior leadership or executive team has little awareness of, or pays little attention to, privacy and its management. | Type rating here |
| **Foundational:** The privacy officer engages with the senior leadership or executive team, governance board and/or committees when there are specific issues and events that need to be addressed. |
| **Managed:** The privacy officer has regular updates and discussions with the senior leadership or executive team, governance board and/or committees on the agency’s privacy culture and values, privacy strategy and programme, and privacy issues and risks. |
| **L1.2** | **Privacy and risk management** | **Informal:** People have an idea of who is responsible for aspects of privacy. Day-to-day functional leadership responsibilities have not been clearly assigned and privacy is not integrated into the agency’s risk management structure. | Type rating here |
| **Foundational:** A senior leader has been assigned responsibility for functional oversight for privacy, though privacy is not integrated into the agency’s risk management structure. |
| **Managed:** Functional oversight for privacy and its work programme is integrated into the risk management organisational structure and includes monitoring compliance. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Leadership 2: Delivery of objectives through management structure, roles and responsibilities, and the capacity to achieve these objectives. | | | |
| **L2.1** | **Responsibility and accountability** | **Informal:** Responsibility and accountability for the implementation of the privacy strategy and work programme are unclear or absent. | Type rating here |
| **Foundational:** The responsibility and accountability for the implementation of the privacy strategy and work programme are seen as the sole responsibility of the privacy officer or team and are not suitably distributed throughout the agency. |
| **Managed:** Formal line management and governance includes responsibility and accountability for the implementation of the privacy strategy and work programme. These responsibilities are suitably distributed throughout the agency. |
| **L2.2** | **Resourcing** | **Informal:** Resourcing for privacy staff and activities is ad hoc and not commensurate with the agency’s privacy profile and privacy work programme. | Type rating here |
| **Foundational:** Resourcing for privacy staff and activities is planned at the individual initiative level. |
| **Managed:** Resourcing for privacy staff and activities is considered at a strategic level within the agency and is commensurate with the agency’s privacy profile and privacy work programme. |
| **L2.3** | **Oversight and visibility** | **Informal:** Privacy activities are ad hoc or reactive. | Type rating here |
| **Foundational:** Because privacy objectives are planned at the individual initiative level, the privacy officer or team does not have sufficient visibility and oversight of the initiatives that need to deliver privacy objectives. |
| **Managed:** The privacy officer or team oversees the privacy work programme, maintains central oversight of privacy initiatives and activities on an agency-wide basis, communicates regularly with other related functions (for example, information management, security, risk management), and has clear alignment (where applicable) with their work programmes. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Leadership 3: Confidence in organisational progress through appropriate monitoring and assurance practices. | | | |
| **L3.1** | **Privacy and assurance** | **Informal:** The privacy risk ownership and responsibilities are reactive and ad hoc. Some controls are functioning to enable timely risk management. The governance group does not have assurance reviews about its controls and risk management processes. | Type rating here |
| **Foundational:** The privacy risk ownership and responsibilities are defined in documented practices and processes. The risk management protocols are applied by individual initiatives or teams. The governance group relies on periodic assurance reviews to provide confidence on its controls and risk management processes. |
| **Managed:** Well-functioning controls and assurance mechanisms are in place to enable the ongoing monitoring of privacy risk. The existing systems and processes make it easy to identify a privacy risk early and escalate it in real time to be able to proactively mitigate risk.  The agency has a controlled and measured assurance environment that allows it to continuously learn and refine its internal practices. The governance group is reasonably confident in the agency’s privacy risk management. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

# Planning, policies and practice

[Planning, policies and practice guidance](https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-maturity-assessment-framework-pmaf-and-self-assessments/complete-a-self-assessment/planning-policies-and-practice/)

|  |  |  |  |
| --- | --- | --- | --- |
| Planning, policies and practice 1: Formulate a privacy strategy, a roadmap to bring it to life and a work programme to achieve it. | | | |
| **P1.1** | **Planning** | **Informal:** Privacy planning is ad hoc or reactive to specific events and incidents. | Type rating here |
| **Foundational:** Privacy planning is seen as the domain of the privacy officer or team with little or no connection to the rest of the organisation. |
| **Managed:** Privacy planning:   * includes all areas of the agency * comprehensively addresses the collection, use, storage and security of personal information, and * is flexible to accommodate changes either in the wider business environment or as the result of assurance activity. |
| **P1.2** | **Planning documents** | **Informal:** The agency does not have privacy planning documents (for example, strategy, roadmap and work programme). | Type rating here |
| **Foundational:** The agency has privacy planning documents (for example, strategy, roadmap and work programme) that are reviewed regularly. |
| **Managed:** Privacy planning documents (for example, a strategy, roadmap and work programme) are:   * easy to understand * communicated to those with relevant responsibilities, and * reviewed regularly to ensure that they remain relevant and aligned with the agency’s organisational and system context (nature, scale and risk). |
| **P1.3** | **Reporting** | **Informal:** Reporting is ad hoc and is about specific events and incidents. | Type rating here |
| **Foundational:** Progress towards their privacy strategy, roadmap and work programme is reported to senior leadership and relevant governance bodies on an initiative basis. |
| **Managed:** Progress towards their privacy strategy, roadmap and work programme is tracked and reported regularly to senior leadership and relevant governance bodies. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Planning, policies and practice 2: Have policies to equip managers and staff to play their part in achieving the core expectations. | | | |
| **P2.1** | **Policies** | **Informal:** Privacy policies and related documents are insufficient to meet the agency’s privacy needs, are communicated in an ad hoc or reactive basis and are not regularly reviewed. | Type rating here |
| **Foundational:** Privacy policies and related documents meet the agency’s privacy needs.  They are used by individual initiatives or within a subset of core business processes (such as procurement, policy or service design, frontline operations and management, analysis and research) but are not explicitly aligned to agency needs. |
| **Managed:** Privacy policies and related documents are easy to understand, communicated and accessible throughout the agency, and reviewed regularly to ensure that they remain relevant and aligned with the agency’s needs. |
| **P2.2** | **Procurement contracts** | **Informal:** The inclusion of privacy policies in procurement contracts is ad hoc or reactive. | Type rating here |
| **Foundational:** The agency’s procurement contracts sometimes include terms and conditions relating to privacy policies and practices, but this happens at the individual initiative level and is not a standard practice. |
| **Managed:** The agency’s procurement contracts include standard terms and conditions relating to privacy, and privacy policies and related documents include advice on external suppliers and personal information. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

# Privacy domains

[Privacy domains guidance](https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-maturity-assessment-framework-pmaf-and-self-assessments/complete-a-self-assessment/privacy-domains/)

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy domains 1: Require a clear understanding of the purpose and necessity of the collection, use or sharing of personal information. | | | |
| **PD1.1** | **Defining the purpose** | **Informal:** The agency’s advice on defining the purpose for the collection, use or sharing of personal information is ad hoc or reactive. | Type rating here |
| **Foundational:** The agency’s guidance on defining the purpose for the collection, use or sharing of personal information is focused on compliance and risk. |
| **Managed:** The agency’s guidance is appropriately aligned with DPUP’s good-practice advice to accurately define purposes for collection, use or sharing of personal information for projects and business processes. |
| **PD1.2** | **Identifying choices** | **Informal:** It’s unusual to offer any choices to service users, and if it is done, it’s ad hoc or reactive. | Type rating here |
| **Foundational:** Steps to identify practical choices that service users may be given regarding the collection or use of their personal information are taken by individual initiatives. |
| **Managed:** Additional processes are explicitly applied to identify when and how choices may be offered or accommodated when appropriate, aligning with DPUP’s good-practice advice. |
| **PD1.3** | **Reducing personal information** | **Informal:** Any steps to reduce or eliminate the need for collection or use of personal information are applied on an ad hoc or reactive basis. | Type rating here |
| **Foundational:** Steps to reduce or eliminate the need for the collection or use of personal information are taken by individual initiatives. Existing practice is rarely re-examined. It’s generally assumed that if information is being collected, it’s still reasonable to collect it. |
| **Managed:** When creating or updating a service or process, consideration is given to eliminating or reducing the need for personal information by ensuring that its collection, use and sharing are needed to accomplish the stated outcomes. Existing practice is not used as a justification for continued collection and use. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy domains 2: Ensure the use and storage of personal information protects against inappropriate access, use and modification, while also ensuring effective and efficient support for its intended use. | | | |
| **PD2.1** | **Implementing Privacy by Design** | **Informal:** Privacy, ICT, information management and other responsible teams work in silos when building and updating processes, products and services. | Type rating here |
| **Foundational:** Privacy, ICT, information management and other responsible teams have limited engagement when building and updating processes, products and services. |
| **Managed:** Privacy, ICT, information management and other responsible teams work together to incorporate Privacy by Design methodology and principles when building and updating processes, products and services. |
| **PD2.2** | **Implementing privacy engineering** | **Informal:** Privacy and ICT staff have no knowledge and understanding of using privacy engineering to address privacy considerations. | Type rating here |
| **Foundational:** Privacy, ICT and digital teams may have some knowledge and understanding of using privacy engineering to address privacy considerations. When building and updating processes, products and services, individual initiatives work with privacy, ICT and digital teams to incorporate privacy engineering and privacy design strategies. |
| **Managed:** Privacy, ICT and digital teams have sufficient knowledge and understanding of using privacy engineering to address privacy considerations. When building and updating processes, products and services, privacy, ICT and digital teams work together to incorporate privacy engineering. |
| **PD2.3** | **Responding to high public interest** | **Informal:** When considering or piloting uses of personal information that would attract high public interest, such as biometrics or automated decision-making, policies and practices are reactive and non-specific. | Type rating here |
| **Foundational:** When considering or piloting uses of personal information that would attract high public interest, such as biometrics or automated decision-making, existing policies and practices have been adapted by individual initiatives to consider such forms of use. |
| **Managed:** When considering or piloting uses of personal information that would attract high public interest, such as biometrics or automated decision-making, specific policies and practices have been developed or identified to address concerns and consideration of such forms of use. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy domains 3: Make it easy for people to access and request correction to their information. | | | |
| **PD3.1** | **Having a process** | **Informal:** The approach to responding to access requests is ad hoc or reactive, and it’s not easy for clients to find or understand how to do this. | Type rating here |
| **Foundational:** Customers and clients can find a process to make an access request, but it’s not clear if they find it easy to use. |
| **Managed:** Customers and clients can easily find and understand the process to make an access request. |
| **PD3.2** | **Monitoring the process** | **Informal:** Access request responses are done on an ad hoc basis with no systematic monitoring. | Type rating here |
| **Foundational:** The agency has an access request process. The requesters and the agency have little visibility of whether the access requests responses are meeting the legislative requirements. |
| **Managed:** The agency has a people-centred access request process that aligns with DPUP’s good-practice advice on access to personal information.  The agency monitors and ensures that access request responses meet the legislative requirements and supports the agency’s reputation as an effective and trusted custodian of people’s personal information. |
| **PD3.3** | **Reviewing the process** | **Informal:** Actions to improve the process for responding to access requests are ad hoc or reactive. | Type rating here |
| **Foundational:** The agency relies on individual initiatives to enable timely responses to access requests by considering easy access and collation of personal information. |
| **Managed:** Information management and ICT system reviews explicitly include consideration of easy access and collation of personal information to enable timely responses to access requests. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy domains 4: Understand and assess privacy risks and manage commensurately. | | | |
| **PD4.1** | **Knowing agency risks** | **Informal:** Privacy risks are not assessed or are assessed for specific events and incidents. | Type rating here |
| **Foundational:** Privacy risks are assessed based on little understanding and knowledge of personal information holdings and the collection, uses, sharing activities, and storage of personal information. |
| **Managed:** Privacy risks are assessed based on an understanding and knowledge of personal information holdings (for example, data inventory or stocktake), focusing on collection, uses, sharing activities, and storage. |
| **PD4.2** | **Managing agency risks** | **Informal:** Agency privacy risk assessments, which provide a snapshot of an agency’s current privacy risks, are not done. | Type rating here |
| **Foundational:** Agency privacy risk assessments, which provide a snapshot of an agency’s current privacy risks, are siloed within the privacy team and are not part of the agency’s overall risk assessment. |
| **Managed:** Agency privacy risk assessments, which provide a snapshot of an agency’s current privacy risks and how it will manage them as an organisation, are part of the agency’s overall risk assessment, and are conducted and reviewed periodically. |
| **PD4.3** | **Managing project risks** | **Informal:** Project risk assessments, which are done to assess the privacy risk of new or updated processes, products or services, are done occasionally or not at all. The privacy team has little or no visibility of project privacy risks. | Type rating here |
| **Foundational:** Project risk assessments are done to assess the privacy risk of new or updated processes, products or services. Oversight by the privacy team and associated lines of ownership and accountability are not clear. |
| **Managed:** Project risk assessments are done to assess the privacy risk of new or updated processes, products or services with the support of and oversight by the privacy team. They cover the whole information life cycle and have clear lines of ownership and accountability. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy domains 5: Reduce the impact of privacy breaches and incidents through good privacy practices. | | | |
| **PD5.1** | **Having a privacy incident register** | **Informal:** The agency may have a privacy incident register and/or a privacy incident response plan. Neither are reviewed regularly. | Type rating here |
| **Foundational:** The agency has a privacy incident register and a privacy incident response plan. Learning from privacy incidents and breaches is done by individual initiatives. |
| **Managed:** The agency has:   * a privacy incident register that is used by staff and/or privacy team * a tested privacy incident response plan (including partners and third parties) that is integrated into its business continuity planning * a process for learning from privacy incidents and breaches. |
| **PD5.2** | **Minimising collection of personal information** | **Informal:** Consideration of whether personal information needs to be collected is based solely on compliance and risk assessments. | Type rating here |
| **Foundational:** Consideration of whether personal information needs to be collected and whether there are alternative ways to accomplish the desired outcome may be done by individual initiatives. Little or no review of the personal information already being collected is done when updating a process, product or service. |
| **Managed:** The agency collects only personal information that is clearly linked to the desired outcome and investigates alternative ways to accomplish the desired outcome that eliminates or reduces the need for personal information. |
| **PD5.3** | **Retaining personal information** | **Informal:** The retention and destruction of personal information is done on an ad hoc basis. | Type rating here |
| **Foundational:** The agency has information policy and practices that include the retention and destruction of personal information. |
| **Managed:** The agency has, maintains and promotes information policy and practices that include the retention and destruction of personal information, and this destruction of personal information is authorised by the government’s Chief Archivist. |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy domains 6: Enable personal information use, reuse and sharing to support a unified public service that provides the public with effective services. | | | |
| **PD6.1** | **Having policies for sharing personal information** | **Informal:** Decisions to re-use or share personal information are made operationally and on an ad hoc or reactive basis. | Type rating here |
| **Foundational:** Individual initiatives decide whether and how to re-use or share personal information, and this is primarily seen as a risk-based decision. |
| **Managed:** Information management and privacy policies include enabling advice on how to appropriately use and share personal information when individuals can be identified.  These policies also refer to relevant external sources (for example, information to support tamariki wellbeing, information sharing under the Family Violence Act 2018). |
| **PD6.2** | **Understanding the use of non-personal information** | **Informal:** Sharing of non-personal information is ad hoc or reactive. | Type rating here |
| **Foundational:** Individual initiatives take steps for the respectful, trusted and transparent use, reuse and sharing of non-personal information that does not identify individuals (for example, data and data sets, analysis, qualitative or quantitative information, statistics, research, reports or studies). Privacy and other relevant policies may contain little or no guidance on this topic. |
| **Managed:** Privacy and other relevant policies incorporate advice for the respectful, trusted and transparent use, reuse and sharing of non-personal information that does not identify individuals (for example, data and data sets, analysis, qualitative or quantitative information, statistics, research, reports or studies). |
| **Context:** | (insert comment here) | | |
| **Achievement:** | (insert comment here) | | |
| **Future focus:** | (insert comment here) | | |
| **Challenge:** | (insert comment here) | | |