Te Tari Taiwhenua
Internal Affairs

Digital Economy and Communications briefing

Hon Dr David Clark
Minister for the Digital Economy and Communications

Title: **GCPO report on privacy maturity in the public service: 2022**

Date: 26 October 2022

Key issues
Every year by 30 June, public agencies covered by the GCDO mandate are asked to complete a privacy maturity self-assessment report (PMAF) and return it to the Government Chief Privacy Officer (GCPO). 44 out of 45 agencies completed the 2022 PMAF. By analysing the PMAF returns, the GCPO has identified four key areas where agencies should target privacy improvements over the coming year: resourcing; governance; being better Treaty partners (eg taking a te ao Māori approach to privacy); and training.

Action sought	Timeframe
Note that the overall state of measured privacy maturity is primarily 'Foundational' (evidence of good practice, but at an ad hoc rather than embedded level). This is an encouraging starting point. **Note** that the PMAF returns have informed the GCPO's work programme to help agencies to improve their privacy maturity. **Note** the intention to proactively release this briefing.	DEC officials meeting, 31 October 2022

Contact for telephone discussions (if required)

Name	Position	Contact Number	Suggested 1st contact
Katrine Evans	Government Chief Privacy Officer	0211750342	✓
Ann-Marie Cavanagh	Deputy Chief Executive Digital Public Service and the Deputy Government Chief Digital Officer	021 730 217	

Return electronic document to:	Daniel Anderson, Daniel.Anderson@dia.govt.nz
Cohesion document reference	EEJU23W3HNHT-301358695-82
Ministerial database reference	DEC202200371

For Minister's office:	☐ Seen	☐ Approved	☐ Declined	☐ Withdrawn	☐ More information required

Purpose

1. The purpose of this briefing is to inform you about the state of privacy maturity in the public service for 2022 as measured by the Government Chief Privacy Officer (GCPO).
2. It includes information about areas where development most appears to be needed, and which the GCPO has highlighted to agencies.
3. It also notes how the insights from the 2022 PMAF have also informed the GCPO's work programme, so that we can help agencies to improve their privacy maturity.

Background

4. The GCPO asks the public service agencies that fall within its mandate to report on their privacy maturity by the end of June every year using the PMAF.
5. The previous PMAF was set up 2016, but its focus on legal compliance no longer represented modern privacy programme management, and it has been replaced.[1] This is the first time that agencies have reported against the new Framework, so this briefing represents a **new baseline** for agencies.
6. 45 agencies were asked to complete a PMAF return for 2022. Of these, 44 agencies provided a response, which is the highest rate of return ever achieved. **Appendix A** lists all agencies asked to complete a PMAF self-assessment return in 2022.
7. The PMAF does not focus simply on compliance with the Privacy Act. It sets out a wide range of other measures that are necessary for agencies to handle personal information respectfully and safely.
8. It has four sections (Core Expectations, Leadership, Planning, Policies and Practice, and Privacy Domains) and is aligned with the Cabinet-endorsed Data Protection and Use Policy (DPUP).
9. There are three levels of privacy maturity: Informal, Foundational, and Managed. The Framework sets out in detail what Informal, Foundational and Managed look like for each specific element, so that agencies can respond as consistently as possible. The maturity levels are as follows:
    - 9.1 **Informal**: an agency's approach to privacy is unstructured, privacy is generally seen as compliance only, and there is a need to better plan and implement the agency's privacy activities.
    - 9.2 **Foundational:** an agency-wide approach to privacy is developing, good practice occurs in siloes but not at the wider agency level, and any privacy work programme is driven by individual activities rather than being more embedded in agency-wide practice.
    - 9.3 **Managed:** an agency's approach to privacy is reasonably comprehensive, good privacy practice is part of the agency's culture, and planning and implementing the agency's privacy activities are strategic and appropriately resourced.
10. GCPO asked agencies to include comments in their reports about their successes, challenges and areas for future focus. We received just under 2,000 comments, which we have used to develop insights into the current state of public service privacy maturity, including target areas for development.

[1] Refer DEC202200053 dated 14 March 2022 for more information on the development of the new PMAF.

11. Each agency's Chief Executive and privacy team received an individual report on Thursday 13 October, showing insights for that agency, as well as the system-level insights. These individual reports show agencies how they compare to other agencies. These reports are designed to help agencies to identify areas where they most want or need to prioritise improvements.

12. We have also used the system-level insights to inform the GCPO's own work programme so that we target activities that assist agencies to improve.

Key findings

13. **The majority of agencies reported their privacy maturity for the four sections of the PMAF as Foundational, with some agencies describing they were partially or fully Managed** (figure 1). Only 5% of total privacy maturity indicators (10 of 176) were Informal. This is an encouraging result.

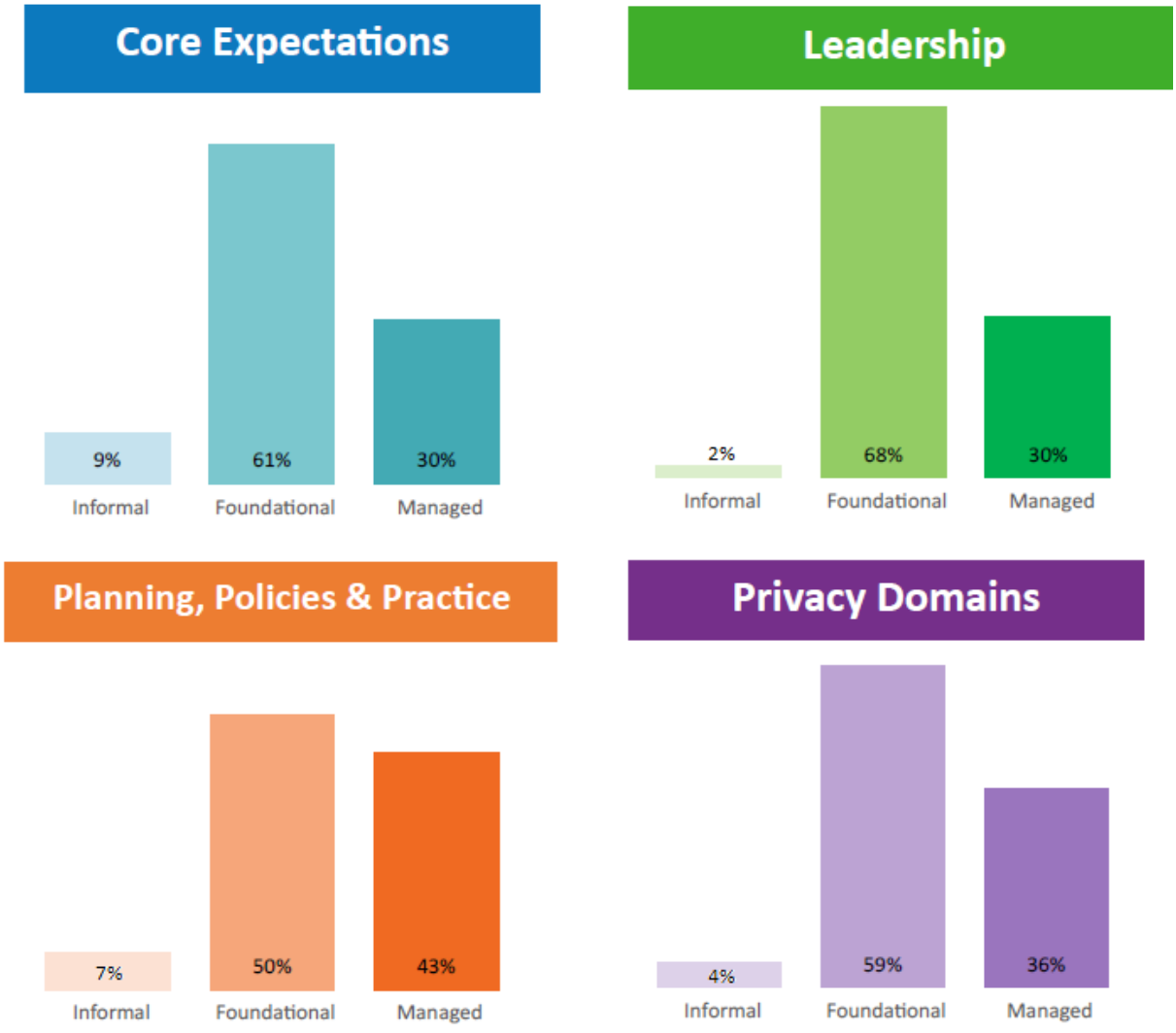


Figure 1: Overview of public service privacy maturity measured 2022

14. **Over time the GCPO expects more and more agencies to reach Managed for their privacy maturity profile.** We expect that next year's results will reflect some improvements, particularly in the specific areas that we have highlighted.

15. However, we do not expect a significant or sudden shift towards Managed across all aspects of the PMAF between reporting years. It is likely to be a gradual process as

growth will need longer-term investment in privacy resources and capability. In addition, the time and steps that each agency will take to improve its maturity will be different, depending on the scope of the agency's work, its competing priorities, the existing state of its assets, and the level of risk associated with the information it holds.

16. More detailed results are in **Appendix A** and show privacy maturity results for Category 1 (large agencies with multiple personal information holdings) and Category 2 (small to medium agencies with a single or small number of personal information holdings).

Key messages from the Government Chief Privacy Officer for 2022

17. The GCPO has highlighted four main areas that are key levers for system maturity improvements:

    17.1 **Resource privacy capability adequately** to avoid preventable privacy risks and to build maturity over time. This includes not only resourcing specialist privacy teams, but building capability in other relevant areas, such as service design, IT, and information management, so that the privacy basics are covered without the need for privacy team intervention at every stage.

    17.2 Make sure **privacy issues are visible at the governance level**, that governance groups have the information they need, and that leaders actively promote privacy messages.

    17.3 Agencies are taking a variety of steps to **be better Treaty partners** with how they handle personal information (for example taking account of Māori data sovereignty and te ao Māori perspectives on privacy), but this is an area in which more assistance is required.

    17.4 Many agencies have done **good work with developing privacy training**. Further steps that agencies can take include ensuring those training modules are compulsory for all staff, that training extends beyond induction and is relevant and engaging, and that training is required before access to core personal information systems is provided.

The GCPO's work programme

18. These insights have informed the GCPO's own work programme. For example:

    18.1 We are working with Wellington Uni Professional on a privacy foundational skills micro-credential. The aim is to train new privacy advisers (to help to address the critical skills shortage in the labour market) and also provide staff in other relevant areas of practice with foundational skills.

    The first microcredential course is likely to be available in April 2023.

    18.2 Once the detailed content development is complete for the microcredential (around February 2023), this will free up our time to focus on other ways in which we can develop training or support for new or existing privacy professionals. Options include working with the International Association of Privacy Professionals (the premier global privacy organisation) to develop relevant New Zealand material.

    18.3 We are starting to work with more experienced agencies to share the core resources that they have, such as policies, strategies, roadmap formats, training modules, and basic reporting metrics. The intent is to create a toolkit

of re-usable, editable resources. This will reduce the need for agency privacy officers to build their own resources from scratch. It should particularly benefit small agencies that do not have full-time privacy officers or teams.

We aim to identify a home for such resources and have some key materials included in the toolkit by the end of June 2023.

18.4 In the meantime, we can actively connect agencies that are looking for resources on specific topics with others in the sector who may have something that they can share. Sharing training modules is an area where there can be some immediate benefit.

18.5 While we will continue to provide support and advice to all agencies, we will concentrate on agencies that are struggling with their privacy maturity, to help them develop practical solutions.

18.6 We will continue to engage in the work of the Office of the Privacy Commissioner, system leaders, and others who are leading discussions on Treaty partnerships, Māori data sovereignty, and te ao Māori perspectives on privacy. However, timeframes for that work are not in our control.

PMAF criterion about high-risk uses of personal information

19. The new PMAF includes a criterion asking agencies if they have processes in place to manage new and high-risk uses of personal information, such as biometrics and the impact those technologies have on privacy.

20. Other novel uses of personal information that have gathered some public attention include social media monitoring and the trial of safety cameras identifying mobile phone use by drivers.

21. We are aware that this is a specific area of interest for you, so have included detailed agency results in **Appendix B**.

Next steps

22. You may wish to circulate this briefing to your Cabinet colleagues. We have notified agencies that we are sending you this briefing and that they may wish to discuss their privacy maturity assessment with their Minister.

23. GCDO's normal practice is to **proactively release** briefing papers, as part of the GCPO's existing resources on digital.govt.nz.

24. Officials will be available to discuss this paper at your meeting with Officials on 31 October 2022.

Recommendations

25. We recommend that you:

a) **note** that 44 out of a possible 45 agencies completed the 2022 Privacy Maturity Assessment and provided returns to the GCPO; **Yes/No**

b) **note** that the overall state of measured privacy maturity is primarily Foundational, which is an encouraging starting point; **Yes/No**

c) **note** that the GCPO has identified four major priority areas for agencies to improve: resource privacy teams adequately, raise privacy issues and risks to agency governance groups, become better Treaty partners, and continue improving training for staff. **Yes/No**

d) **note** that the PMAF returns have informed the GCPO's work programme to help agencies to improve their privacy maturity. **Yes/No**

e) **note** the intention to proactively release this report. **Yes/No**

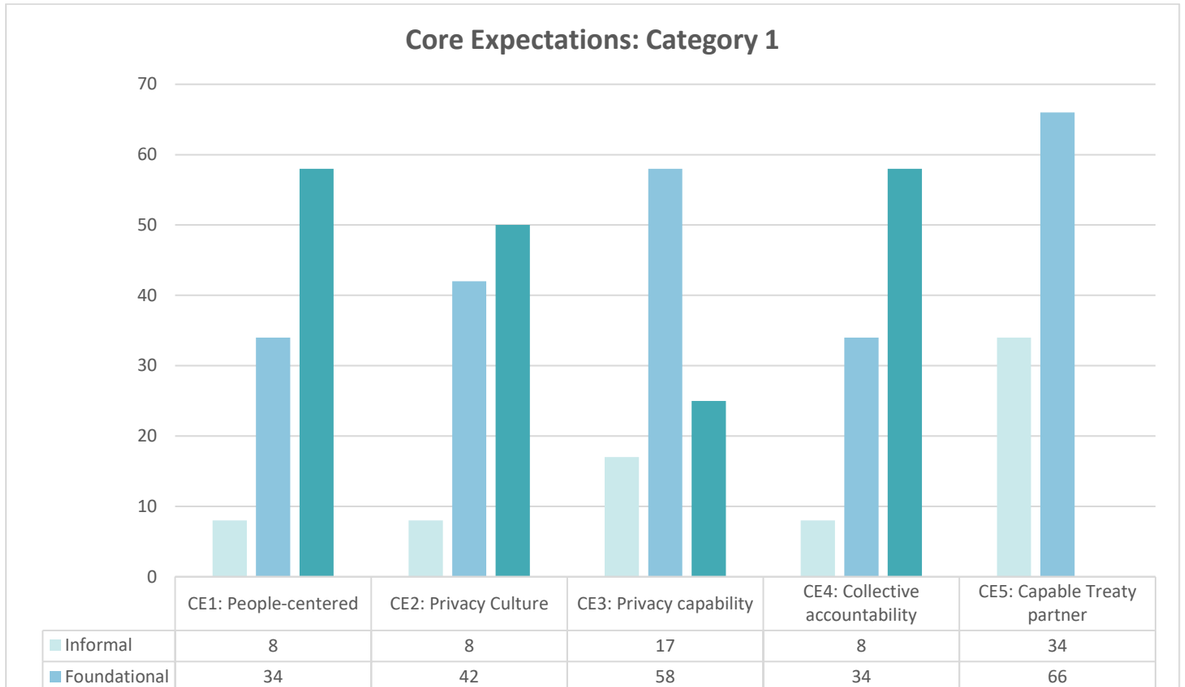
K Evans

Katrine Evans
Government Chief Privacy Officer

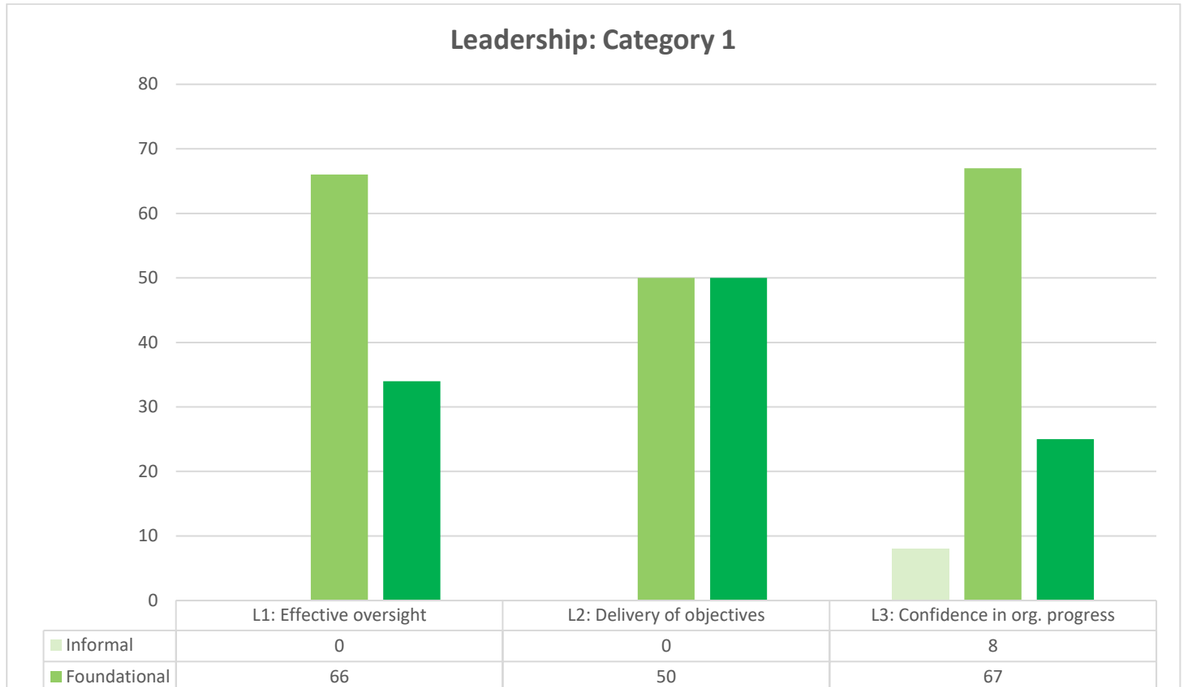
Hon Dr David Clark
Minister for the Digital Economy and Communications
31 / 10 / 2022

Appendix A1: Category 1 results from the 2022 Privacy Maturity Assessment Framework self-reporting returns

Category 1 agencies are the twelve public service departments and Crown agents that have large amounts of personal information and/or use personal information for multiple purposes.

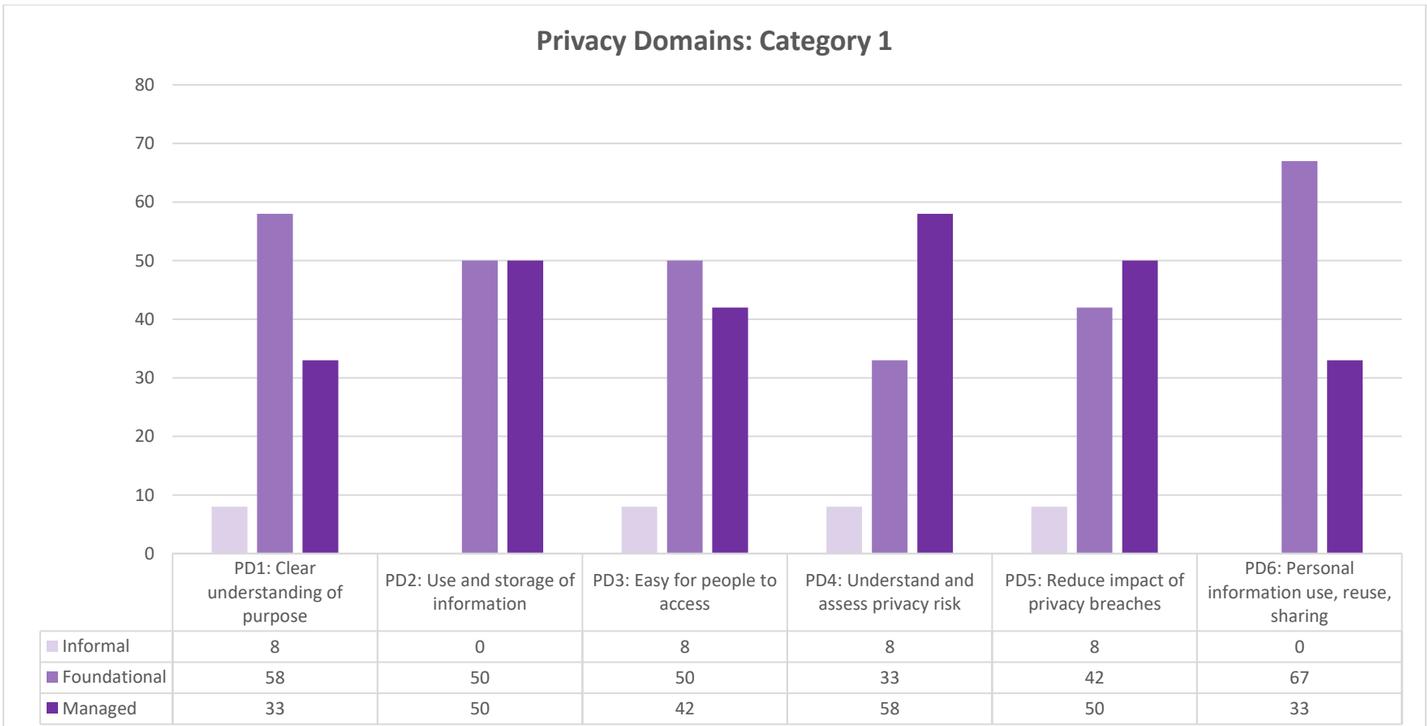


	CE1: People-centered	CE2: Privacy Culture	CE3: Privacy capability	CE4: Collective accountability	CE5: Capable Treaty partner
Informal	8	8	17	8	34
Foundational	34	42	58	34	66
Managed	58	50	25	58	0



	L1: Effective oversight	L2: Delivery of objectives	L3: Confidence in org. progress
Informal	0	0	8
Foundational	66	50	67
Managed	34	50	25

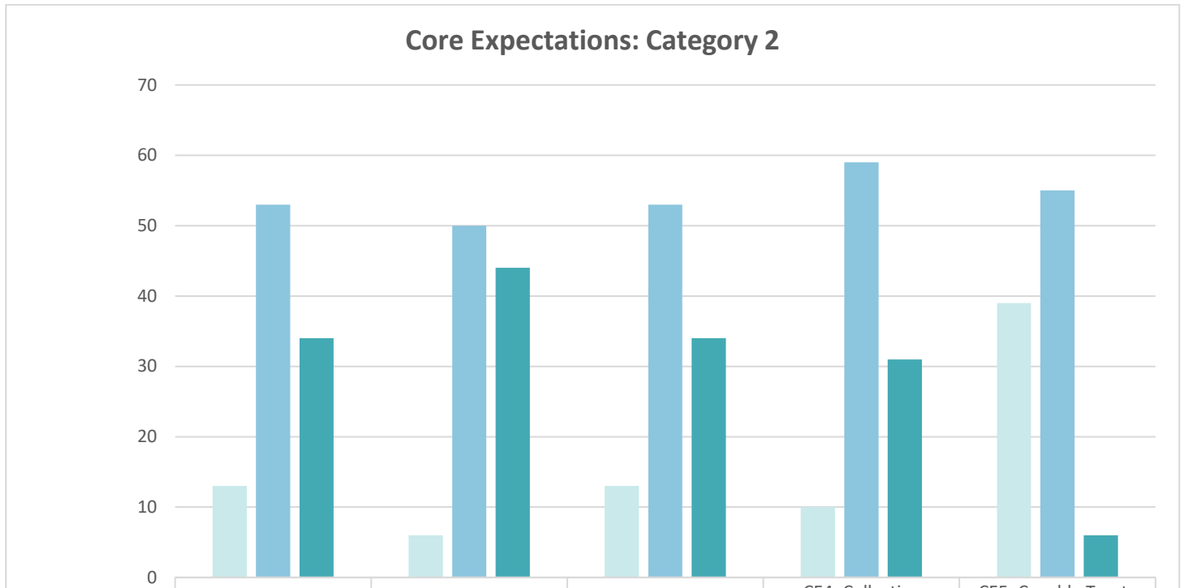
	PPP1: Strategy and planning	PPP2: Competent practice
Informal	8	0
Foundational	42	58
Managed	50	50



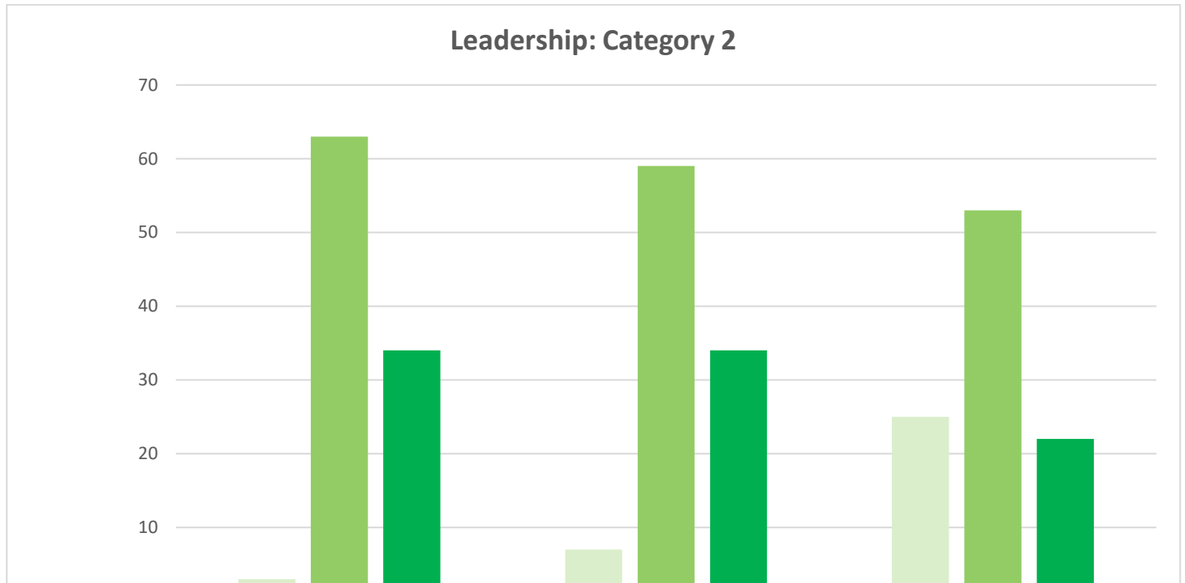
	PD1: Clear understanding of purpose	PD2: Use and storage of information	PD3: Easy for people to access	PD4: Understand and assess privacy risk	PD5: Reduce impact of privacy breaches	PD6: Personal information use, reuse, sharing
Informal	8	0	8	8	8	0
Foundational	58	50	50	33	42	67
Managed	33	50	42	58	50	33

Appendix A2: Category 2 results from the 2022 Privacy Maturity Assessment Framework self-reporting returns

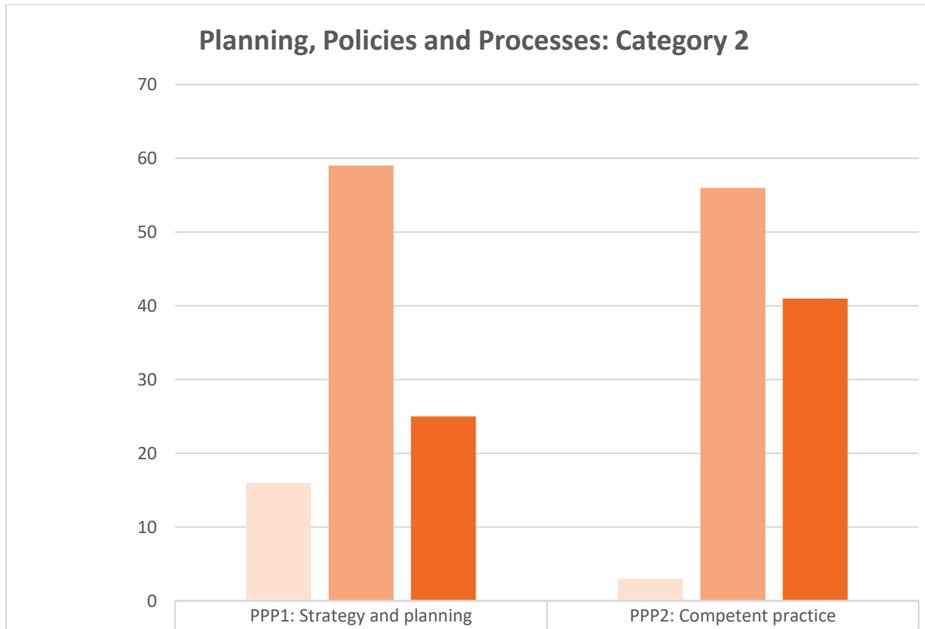
Category 2 agencies are the thirty-three public service departments and Crown agents that have small amounts of personal information and/or only use personal information for one purpose.



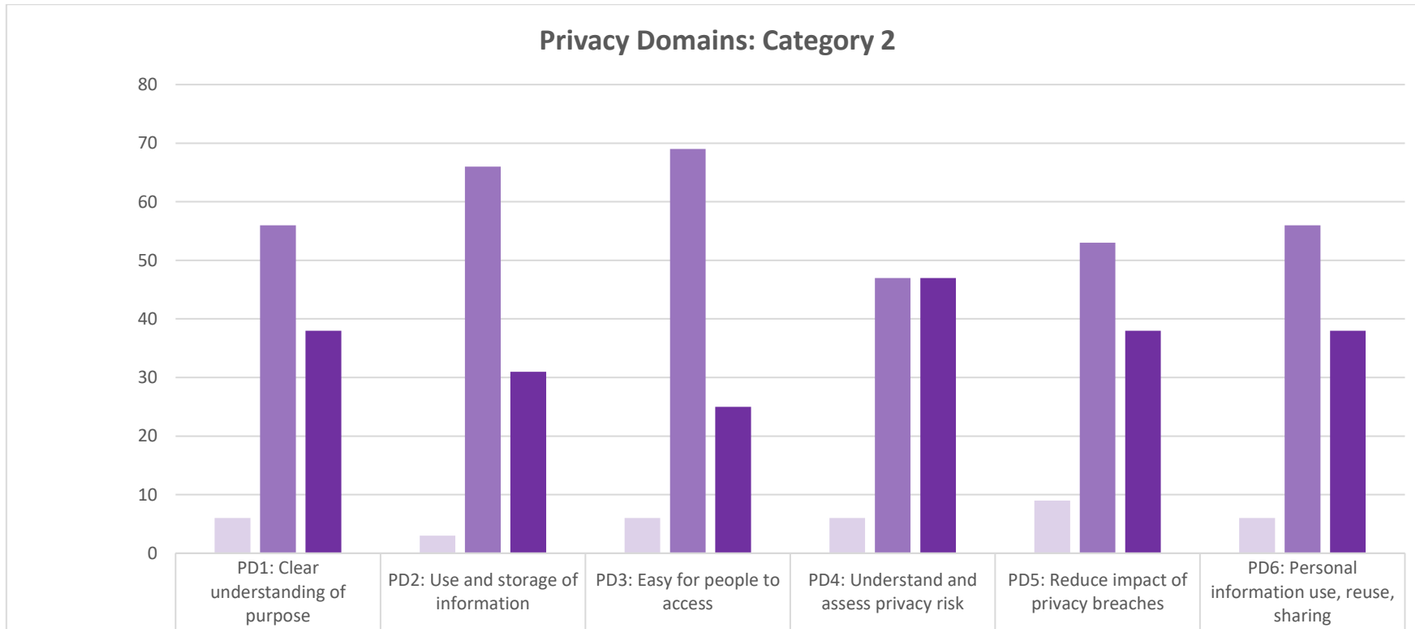
	CE1: People-centered	CE2: Privacy Culture	CE3: Privacy capability	CE4: Collective accountability	CE5: Capable Treaty partner
Informal	13	6	13	10	39
Foundational	53	50	53	59	55
Managed	34	44	34	31	6



	L1: Effective oversight	L2: Delivery of objectives	L3: Confidence in org. progress
Informal	3	7	25
Foundational	63	59	53
Managed	34	34	22



	PPP1: Strategy and planning	PPP2: Competent practice
Informal	16	3
Foundational	59	56
Managed	25	41



	PD1: Clear understanding of purpose	PD2: Use and storage of information	PD3: Easy for people to access	PD4: Understand and assess privacy risk	PD5: Reduce impact of privacy breaches	PD6: Personal information use, reuse, sharing
Informal	6	3	6	6	9	6
Foundational	56	66	69	47	53	56
Managed	38	31	25	47	38	38

Appendix A3: List of which agencies are in each category

Category 1		
Accident Compensation Corporation	Ministry of Business, Innovation and Employment	New Zealand Customs Service
Department of Corrections	Ministry of Education	New Zealand Police
Department of Internal Affairs	Ministry of Justice	Oranga Tamariki
Inland Revenue	Ministry of Social Development	Waka Kotahi New Zealand Travel Agency

Category 2		
Crown Law Office	Ministry for the Environment	New Zealand Trade and Enterprise
Department of Conservation	Ministry for Women	Office of the Clerk of the House of Representatives
Department of Prime Minister and Cabinet	Ministry of Defence	Parliamentary Service
Earthquake Commission	Ministry of Health	Parliamentary Counsel Office
Education Review Office	Ministry of Transport	Te Kawa Mataaho Public Service Commission
Government Communications Security Bureau	Ministry for Primary Industries	Serious Fraud Office
Ministry of Housing and Urban Development	Ministry for Pacific Peoples	Statistics New Zealand
Kāinga Ora Homes and Communities	National Emergency Management Agency	Social Wellbeing Agency
Land Information New Zealand	New Zealand Defence Force	Te Puni Kokiri
Ministry for Culture and Heritage	New Zealand Qualifications Authority	Tertiary Education Commission
Ministry of Foreign Affairs and Trade	New Zealand Security Intelligence Service	Treasury

Appendix A4: Privacy Maturity Assessment Framework elements

Core Expectations:

CE1: **Take a people-centred approach** to privacy that is respectful of those the information is about and provides the public with effective services.

CE2: **Build and maintain a privacy culture** that embodies the public service values of being impartial, accountable, trustworthy, respectful and responsive.

CE3: **Build and maintain privacy capability** so that people have the knowledge and skills they need to contribute to good privacy practice.

CE4: **Establish a sense of collective accountability** in which managers and staff understand their duty to ensure that personal information is collected and used appropriately.

CE5: **Be a capable Treaty partner** by supporting the Crown to fulfil its stewardship responsibility and strengthen Crown's relationships with Māori.

Leadership

L1: **Effective oversight** for privacy practice through effective governance.

L2: **Delivery of objectives** through management structure, roles and responsibilities, and the capacity to achieve these objectives.

L3: **Confidence in organisational progress** through appropriate monitoring and assurance practices.

Planning, policies, and processes

PPP1: **Strategy and planning:** Formulate a privacy strategy, a roadmap to bring it to life and a work programme to achieve it.

PPP2: **Competent practice:** Have policies to equip managers and staff to play their part in achieving the core expectations.

Privacy domains

PD1: **Require a clear understanding of the purpose** and necessity of the collection, use or sharing of personal information.

PD2: **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.

PD3: **Make it easy for people to access** and request correction to their information.

PD4: **Understand and assess privacy risks** and manage commensurately.

PD5: **Reduce the impact of privacy breaches** and incidents through good privacy practices.

PD6: **Enable personal information use, reuse and sharing** to support a unified public service that provides the public with effective services.

Appendix B: New criterion: areas of high risk or high public interest (eg new technology use)

1. As mentioned at paragraph 19, a new criterion was introduced to the PMAF to measure privacy maturity of agencies engaging in practices that can create a high level of public interest, such as facial recognition technologies or other new technologies.

2. This criterion sets expectations that **agencies will have sound ways to manage risks associated with practices that may attract a high public interest.** Over time, it should also provide valuable information about how certain technologies are being implemented in the public sector.

3. To assess itself as "Managed" an agency must demonstrate the following:

> *"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."*

4. Examples of such policies and practices would include completing and publishing a Privacy Impact Assessment approved by senior agency leadership. Guidance associated with this question points specifically to resources such as the biometrics position paper from the Office of the Privacy Commissioner[2], having a governance structure on new technology use, implementing the *Guiding Principles for the Use of Biometric Technologies*, or any other type of current policy or standard.

5. Privacy officers completing the self-assessment returns had their attention specifically brought to this new criterion during workshops and consultation sessions as it was the only new criterion added to the PMAF following the beta test in 2021.

6. **Of 44 agencies responding, 19 (43%) said they were Managed, 16 (37%) said they were Foundational, and 9 (20%) said they were Informal.**

    6.1 Fifteen agencies provided no comment relating to this criterion.

    6.2 A further ten agencies explicitly stated that they do not engage in activities using personal information that would gather high public interest such as biometrics. These responses all came from Category 2 agencies with limited personal information holdings.

    6.3 Amongst the twelve Category 1 agencies, four did not provide any comments. The remaining eight mentioned initiatives that are relevant to this criterion, including the New Zealand Traveller Declaration at New Zealand Customs Service, the high wealth individual research project at Inland Revenue, the Data Science Review Board at MBIE, the Automated Decision-Making Standard at MSD, and the Emerging Technology Framework and Working Group at New Zealand Police.

        6.3.1 Seven of the twelve Category 1 agencies measured themselves as Managed, four were Foundational, and one was Informal.

[2] Refer DEC202100345 dated 21 October 2021 for more information on the Privacy Commissioner's position paper on biometrics.

7. We expect maturity to improve with this criterion as additional guidance on uses of personal information that will attract a high level of public interest is developed. The most obvious example is the work that the Office of the Privacy Commissioner is doing relating to biometrics regulation, including potentially developing a code of practice.
8. However, we expect some Category 2 agencies to continue reporting as Informal for some time. If they are not currently planning to implement such technologies, it is unlikely that improving privacy maturity in this space will be a major priority for them, compared with other maturity improvements they wish to make.