TE TAUNAKI
Public Service Census
2021

Te Kāwanatanga o Aotearoa
New Zealand Government

Te Taunaki | Public Service Census 2021

Privacy Impact Assessment Report

Author: Jacinta Coe, Data Engineer, Strategic Information Team, Te Kawa Mataaho

Document Status: Final

Last updated: 24 March 2021

Contents

1. Project summary: Te Taunaki | Public Service Census

Te Kawa Mataaho is conducting a census of employees in 36 Public Service departments and departmental agencies in May 2021.

The purpose of Te Taunaki is to gather information to better understand:

- the diversity of public servants, and their inclusion and wellbeing at work
- experiences of, and views on, working for the Public Service to support a unified Public Service that delivers effectively for Aotearoa and its people.

The main objectives of the census are:

1. To better understand inclusion and diversity in New Zealand's Public Service and gauge how well this diversity reflects the communities we serve.
2. To better understand how public servants' diversity, inclusion and wellbeing at work are supported by employment conditions and working arrangements in the Public Service.
3. To identify how agencies can best support public servants to perform most effectively in their jobs and any barriers that may exist.
4. To better understand public servants' motivations for working for the Public Service.
5. To gather baseline information that can be used to assess progress on elements of the Public Service reforms.

We have decided on a **centralised model for the first Public Service Census, Te Taunaki** where our Strategic Information team (SIT) will work with our selected research provider Research New Zealand (RNZ) to deliver the census, collecting responses from public servants within participating agencies, rather than using a model where public service agencies are responsible for delivering the census.

The census will be primarily administered online, with the aim of an average online completion time of about 15 minutes. Other data collection modes may be used such as telephone and postal/ hard copy as required by certain groups of respondents (eg, Department of Conservation field staff).

Participation in the census will be voluntary, but strongly supported by participating agencies. We are intending to capture 'new starters' by requesting weekly updates of email addresses from agencies for any new starters.

It is intended that the census be repeated every two years, so that we can monitor the overall health of New Zealand's Public Service over time. In the future, the census coverage may be extended beyond core public service agencies to the wider public sector. If the scope of the census does change another Privacy Impact Assessment (PIA) will be completed to ensure any risk of doing so are identified.

The purpose of doing this PIA is to ensure privacy requirements are considered and applied to Public Service Census processes, methodology and reporting. Through completing this PIA we identify any potential risks arising from the collection, use or handling of personal information.

Te Kawa Mataaho has processes and practices in place to ensure privacy is maintained. These include:

- Having a chief privacy officer who supports the business upholding our privacy requirements.
- Completing an Annual Privacy Self-Assessment Assurance Report to ensure we continue to uphold and improve our privacy practices throughout the organisation.
- Maintaining a risk register to ensure any potential issues are identified and mitigated.
- Having an Information Strategy which underpins our decision making when managing our strategic information.

2. Scope of the PIA

Te Taunaki will be delivered to approximately 60,000 public servants working in 36 Public Service departments and departmental agencies (see Appendix 1), including any offshore based New Zealand staff.

This PIA covers the following processes:

- Te Kawa Mataaho obtaining respondents' details from 36 Public Service agencies and sharing this with RNZ so that they can invite respondents to participate in the census and monitor responses for targeted reminders and response rates.
- RNZ creating the survey hosted on their secure platform, collecting individual responses.
- RNZ producing a clean, raw anonymised unit record dataset for Te Kawa Mataaho.
- E-Reporting tool set up and administration for agencies to view their aggregated results against system level results.
- Te Kawa Mataaho producing system level reporting.

To ensure these processes are conducted successfully the following aspects of the information collection have been further documented below:

- Tools and systems
- Data management
- Use of the information
- Data transfer
- Storage
- Access
- Reporting
- Retention and disposal

Tools and systems

The census information collection requires the use of the following systems and tools:
Internal:

- MS Outlook (email using SEEMail tag)
- MS Groups (SFTP (accessed via MS Authenticator)) – Office365 Certified
- Power Automate – Office365 Certified
- MS Excel – Office365 Certified

- Python (programming language)
- MS SQL server – Going through accreditation
- Tableau – Going through accreditation
- NVIVO (qualitative analysis).

External:

- Survey tool (Voxco)
- E-Reporting tool (hosted on RNZ secure server).

Data management

Te Kawa Mataaho have an information strategy, which sets out the high level context for managing our strategic information resources. At the heart of the strategy are four principles that underpin our decision making when managing our strategic information.

The four principles are:

- Information into insight: Information supports Te Kawa Mataaho to monitor, design and evaluate the performance of the public sector
- Information is an asset: Information should be seen as an asset of Te Kawa Mataaho so that it is managed and used to realise its full value to Te Kawa Mataaho.
- Information is well managed: Information is managed efficiently and effectively and can be trusted as being accurate
- Information is protected and open: Information held by Te Kawa Mataaho should be proactively shared across the agency and with the public unless there are grounds for refusal, such as for personal, confidential or classified information

The principles are built into Te Kawa Mataaho practice through four functional areas, where we look to ensure information is managed well, able to realise full value from it through analysis and sharing of our data, information and insights.

The information polices and protocols under our Information Strategy are:

- Information Management Protocols
- Information Release Protocol
- Information Collections Guidelines
- Confidentiality Guidelines
- Information Roles and Responsibilities

At the heart of these policies and protocols is privacy and security of our information. It is important anyone handling strategic information is made aware of their obligations to manage that information appropriately.

RNZ have Data and Sample Security Policies and Practices in place to ensure they meet their requirements identified in the New Zealand Information Security Manual. These reflect customer information that is considered to be in-confidence, potentially sensitive and/or restricted.

RNZ's Data and sample Security Policies and Practices cover:

- How they handle files containing customer information
- Access control
- Integration
- Data storage
- Recovery and restoration
- Approach and measure to counter security attacks
- Support
- Physical security
- Policy with regard to off-shore storage.

Use of the information

Information from the census will be used by Te Kawa Mataaho to inform progress on work towards achieving Te Kawa Mataaho's vision (a leading edge, unified, trusted Public Service that serves Aotearoa and its people) and strategic priorities (strong constitutional role; better outcomes and services; modern, agile, adaptive; diverse and inclusive; supporting the Crown in its relationships with Māori under Te Tiriti o Waitangi / the Treaty of Waitangi. Census data will also inform specific workstreams and focus areas such as Spirit of Service, future workforce and Māori-Crown Relationships.

Agencies will be able to compare results for their agency with results at a system-level to help identify where work may be needed to ensure that staff are best supported to deliver on government priorities. Small count suppression will be applied to the results supplied to agencies to maintain confidentiality.

Stakeholders such as Te Arawhiti, Te Puni Kōkiri and Te Taura Whiri i te Reo Māori will be provided with aggregated results for their prioritised information needs. This will likely be cross tabulated by other dimensions with small count suppression applied to maintain confidentiality.

Data transfer

Agencies will email their respondents' details (first name and email addresses) to Te Kawa Mataaho's census email address using SEEMail and In-Confidence tags. Once a file has been received by the agency contact it will be moved into our SharePoint file system (restricted folder).

Files shared between Te Kawa Mataaho and RNZ will be through an MS Group.
Te Kawa Mataaho will set up the MS group to be used for sharing files between us and RNZ. To access, the group users will need to go through MS Authenticator. These groups will also be set up to ensure that only SIT and IT can access the information internally. Once received files will be moved out of the group and into another location. The files we provide to RNZ will be restricted to those researchers working on the project.

Storage

The Census will be hosted on a secure online survey platform Revera, where completed census responses will be sent directly to RNZ via a secure transfer system.

Revera is one of three, government-approved local cloud providers. Revera is required to provide robust security safeguards to protect against unauthorised physical access to all their data centres that host Government ICT services.

Use of this platform will be fully tested and piloted before we go live with Te Taunaki. We have ensured that RNZ has fully secure systems for storing and handling the census data by ensuring they met all security pre-conditions through procurement (Appendix 2) and we have reviewed their survey systems penetration results.

The anonymised unit record census dataset (names and email addresses removed) we receive from RNZ will be imported and stored in Te Kawa Mataaho's secure MS SQL Server database.

Access

To ensure individual's privacy is maintained, Te Kawa Mataaho will restrict access to the final anonymised unit record dataset stored in Te Kawa Mataaho's secure MS SQL Server database. Access will only be used to produce aggregated results for statistical or research purposes. To have this access, a small group of approved researchers will be required to review the Access, Security and Privacy Protocols for the Public Service Census and sign the confidentiality agreement form. The Manager Strategic Information and Deputy Commissioner Strategy and Policy are the only people who can grant access to the anonymised unit record data forming part of Te Taunaki, other than the Public Service Commissioner. Government analysts and other bona fide researchers may request access to anonymised unit record data, for research purposes.

Reporting

Data collected from the census will be aggregated to a Public Service level for public reporting on key measures, such as wellbeing at work for employees within the Public Service. Agencies will also be able, through the e -Reporting tool, to compare results for their agency with results at a system-level. These results will have small data cell sizes suppressed to protect anonymity. Further, any output from research using the final anonymised unit record dataset, will be aggregated, and checked to ensure small data cell sizes are suppressed before it leaves our secure IT environment.

Key contacts in each agency will be set up as users in the e-Reporting tool. The users will be administered by Te Kawa Mataaho SIT who will be set up as an administrator by Research New Zealand.

Retention and disposal

The files we receive from agencies for the purposes of creating a master list to send to RNZ will be destroyed after the census is conducted under General Disposal Authority 7, Class 1.6, as the master list will become the authoritative record. The master list files will be retained for at least

10 years before being transferred to Archives New Zealand, under Te Kawa Mataaho Disposal Schedule, class 8.7[1].

The raw dataset we obtain from RNZ and information/records about the development of the census, methodology, processes and protocols for the collation of results and development of any reports interpreting the results will be retained for at least 10 years before being transferred to archives New Zealand. This is in line with Te Kawa Mataaho Disposal Schedule, classes 8.7 and 8.8.

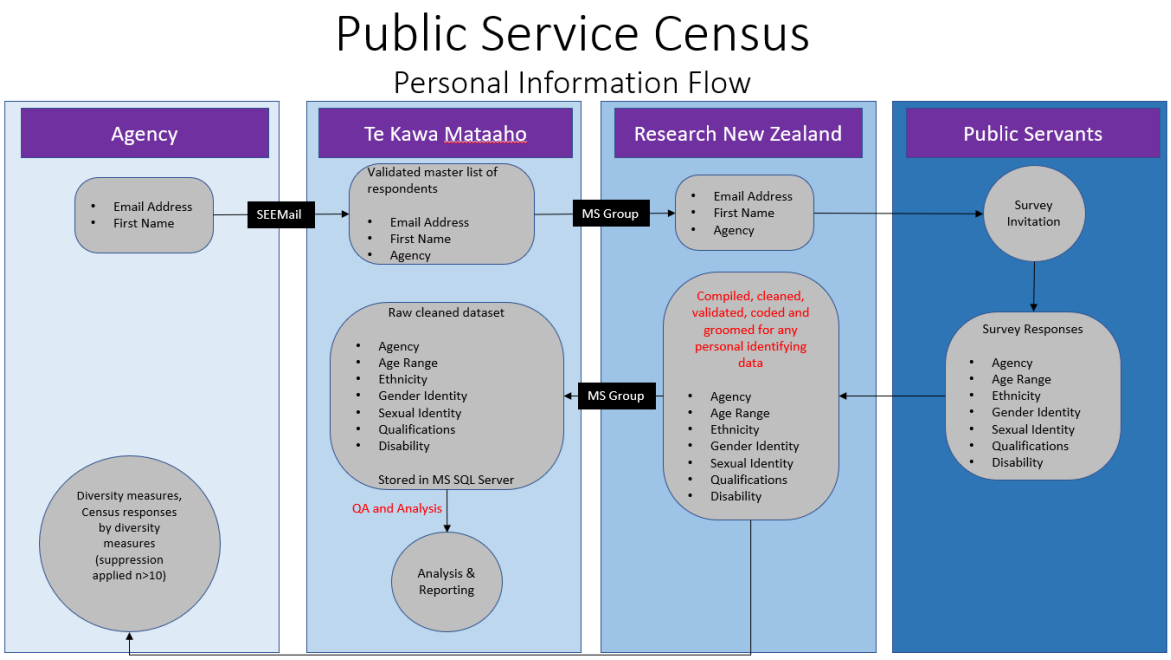
Individual census responses (completed paper surveys) will be destroyed after at least three months of the publication of the system level results under Te Kawa Mataaho Disposal Schedule class 8.9. Te Kawa Mataaho will request RNZ provide written confirmation they have destroyed individual responses within this period.

RNZ remove any data relating to a respondent's identity from any administrative information that is held on that respondent as soon as is practically possible following the completion of the interviewing for a project (ie, the survey data is de-personalised).

RNZ store all digital data **indefinitely, in a depersonalised form** with Revera, local cloud storage provider, which exceeds their minimum requirement of two years required by ESOMAR and RANZ. This does **not** include files of confidential customer information, which is deleted from our system.

3. Personal information

Figure 1



[1] Te Kawa Mataaho Disposal Schedule is currently in the approval phase with Archives New Zealand. Once approved it will become a Disposal Authority, and information can be sentenced against it.

Information provided by agencies to Te Kawa Mataaho (employees email addresses and first names) will be done via email using SEEMail and in-confidence tags before being moved into restricted SharePoint location for the purposes of validating and creating a master list of respondents to send to RNZ. This process will happen several times during the period the Census is open for.

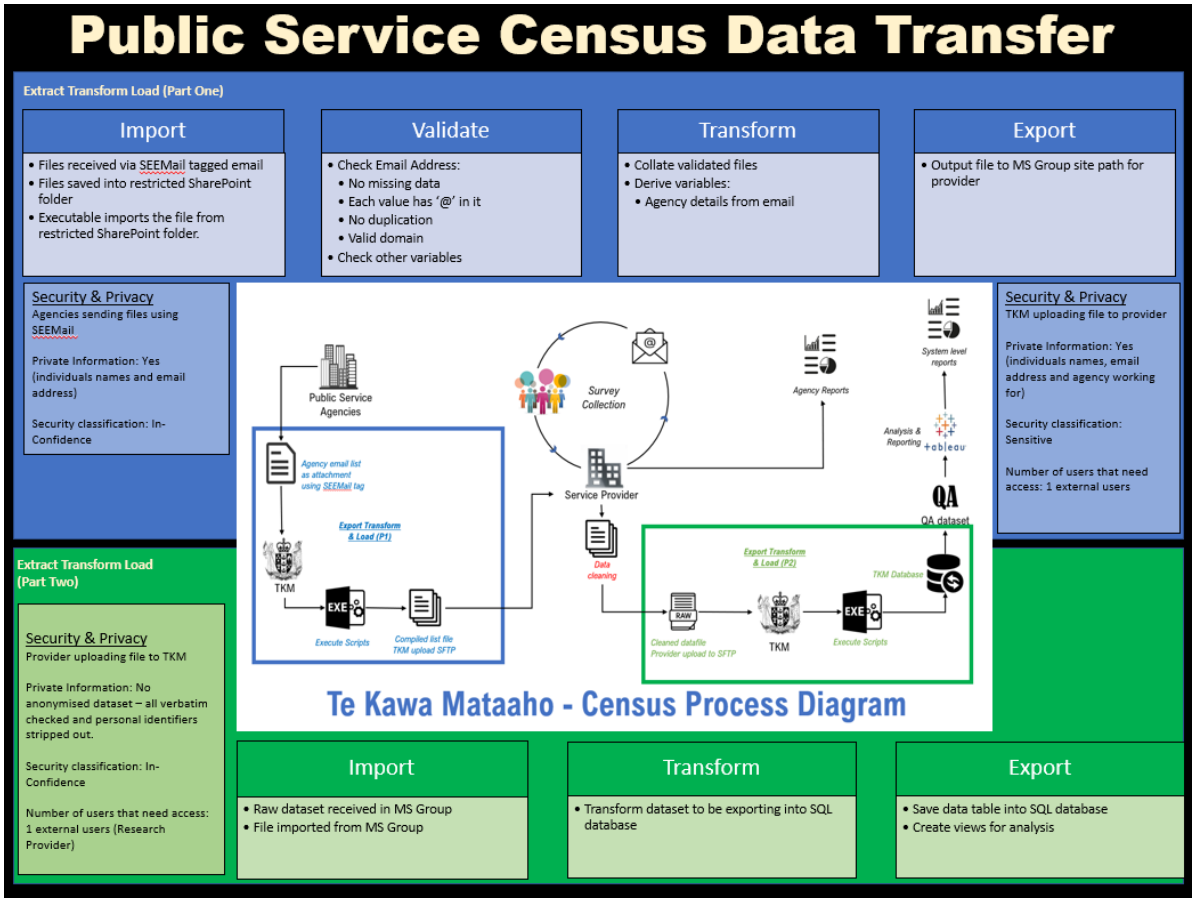
ETL process 1 in Figure 2 below shows the data transfer process from the agencies. Each file is validated, collated and exported to share with RNZ.

RNZ will send individual emails to each respondent with a unique link for them to access the survey. The communication they receive will include an explanation of why we are running a Public Service Census, how their information is going to be used, who will have access to the information and what the benefits are of their participation. There will be links to more information such as the privacy statement (with link to this document) and frequently asked questions which will cover more detail about how their information is going to be managed.

The unit record dataset RNZ provide us with will have gone through a checking process RNZ will complete. The primary purpose of this is to ensure the dataset is anonymised, accurate and complete. This will involve validating, cleaning and coding verbatim responses (including grooming for any personal identifying text).

ETL process 2 in Figure 2 shows the process from RNZ. Te Kawa Mataaho will import the data into our MS SQL Server database before running our own quality checking over the data to test completeness and accuracy.

Figure 2



The e-Reporting tool will be made available to the applicable key contact within each agency. In this tool agencies will be able to compare results for their agency with results at a system-level.

Users that can access this tool will be administered by Te Kawa Mataaho SIT who will be set up as an administrator by RNZ. Te Kawa Mataaho will use their internal information strategy protocols and guidelines to ensure small count suppression will be applied to when needed.

System level reporting will be done on the quality assured dataset. Any agency or demographic breakdowns will require small count suppression. Te Kawa Mataaho will use their internal information strategy protocols and guidelines to ensure reporting is accurate and that no confidential information is released (small count suppressions will be applied when needed).

4. Privacy assessment

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
1	Principle 1 - Purpose of the collection of personal information Only collect personal information if you really need it	Email address – these usually consist of first and last names and the name of the agency the person works for. Only used for collection. Will be removed from the unit record dataset. Demographic Information: Agency worked for Age range Ethnicity Gender identity Sexual identity Qualification Disability The demographic data collected in the census will be used to assess the representativeness of results and to examine how experiences of and views on working for the Public Service differ across groups.	Meets
2	Principle 2 – Source of personal information Get it directly from the people concerned wherever possible	Respondents' email and first name will be provided from the agencies they work at for the purposes of sending invitation for participation and monitoring response. Census responses will be collected directly from people through RNZ secure survey platform. This ensure the responses we get are anonymised and any personal identifying information is removed.	Exception 2/g/ii - will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned
3	Principle 3 – Collection of information from subject Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.	Respondents will be consenting to Te Kawa Mataaho using their data for specified purposes by completing the census. Respondents will be provided with a link asking them to participate in the census. This will come with communication explaining the purpose of census, how their information is going to be used, who will have access to the information and what the benefits are of their participation. There will be links to more information, frequently asked questions which will cover more detail about how their information is going to be managed.	Meets

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
4	Principle 4 – Manner of collection of personal information Be fair and not overly intrusive in how you collect the information	As mentioned in principle 2 – the census responses are collected through RNZ secure survey tool. This ensures the responses we get are anonymised and any personal identifying information is removed. Where possible we have made the demographic dimensions broad. For example, we are using age ranges instead of date of birth or year of birth. Ethnicity is captured at level 3 of the classification which aligns how we report on this information in the Public Service Workforce Data. This option ensures that people are not forced to identify themselves in a more general category.	Meets

5	Principle 5 – Storage and security of personal information
	
	Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.
		Data from agencies will be sent by email with SEEMail and in-confidence tags before being moved into restricted SharePoint location.
		
		The restricted SharePoint location will only be accessible by SIT, this folder will not be discoverable.
		
		The raw dataset uploaded by RNZ to the group site will be there temporarily before being imported into our MS SQL Server Database.
		
		The dataset from RNZ has been groomed, removing email addresses and any personal identifying data.
		
		The MS SQL Server Database sits on secure internal server and is restricted to SIT.
		
		Views of the data for reporting purposes will be extracted and suppression applied where applicable.
		
		Permissions to data sources, groups and the reporting tool will be managed by SIT to ensure only authorised uses can access information.
		
		Te Kawa Mataaho has a number of safeguards to ensure information is well managed. These include:
		
		• Consultancy service Order agreement with RNZ which ensures:
		  ○ That they have met security preconditions (Appendix 2)
		  ○ They agree to participate in any due diligence activities Te Kawa Mataaho undertake to address current or future security risks (penetration testing).
		
		RNZ also have their Data and Sample Security Policies and Practices which outlines:
		• how they handle files containing customer information
		• access control
		• integration
		• data storage
		• recovery and restoration
		• approach and measure to counter security attacks
		• support
		• physical security
		• policy with regard to off-shore storage.
		
		Te Kawa Mataaho has also identified a number of additional safeguards to put in place for this collection:
			Meets with outstanding risks to be mitigated.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
		• Census access protocols • Request for unit record access	
6	Principle 6 – Access to personal information People can see their personal information if they want to	The census dataset will be anonymised with any identifiers removed from the dataset as communicated to respondents on collection and in supporting documentation. Therefore, people cannot see their information.	N/A
7	Principle 7 – Correction of personal information They can correct it if it's wrong, or have a statement of correction attached	As stated above, people cannot see nor correct their information after they have submitted their response.	N/A
8	Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it	Responses will not be altered (except verbatim responses where a person has been named/ identified) however may be suppressed in reporting due to small count size.	N/A
9	Principle 9 – Not to keep personal information for longer than necessary Get rid of it once you're done with it	The files with respondent first name and email used for the purposes of sending invitation to participate in the census will be stored in SharePoint for the duration of census collection then destroyed. The anonymised census dataset and project documentation (including master list files) will be kept for at least 10 years before being achieved. Information about RNZs retention and disposal can be found under scope of the PIA.	Meets

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
10	Principle 10 – Limits on use of personal information Use it for the purpose you collected it for, unless one of the exceptions applies	Comprehensive data is needed to provide a baseline for this system reform from which we can measure progress and get a sense of assurance that the Public Service is moving in the right direction. It will not be used for matching information, at a unit record level, across any other collection. Respondents will be advised that the data will be used for research purposes; it will not be used for any other purposes. Agency level results will be shared with participating agencies through secure e-Reporting tool enabling them to compare their results to system level results. Small cell count suppression will be applied in the tool to protect anonymity.	Meets
11	Principle 11 – Limits on disclosure of personal information Only disclose it if you've got a good reason, unless one of the exceptions applies	N/A	N/A
12	Principle 12 - Disclosure of personal information outside New Zealand	N/A	N/A
13	Principle 13 – Unique identifiers Only assign unique identifiers where permitted	N/A	N/A

5. Risk Assessment

Ref. no.	Aspects of information management	Description of the risk	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk	Recommended mitigations or privacy enhancements	Residual risk remaining despite new safeguards
R-001	Access to raw anonymised data	Users need to have clear understanding of the conditions of their use when accessing the raw dataset which do not currently exist.	Users need to know the conditions of access and consequences of not following the conditions to ensure privacy is maintained	Business has an information strategy which covers all information that comes in and out of Te Kawa Mataaho, however as this is a new collection there are no existing protocols relating specifically to this information.	**Medium**	Access protocols needs to be established with users that have access to raw dataset. These will set out the terms and conditions for use of this data.	**Low**
R-002	Access to raw anonymised data	No established method for internal to request raw dataset access after reviewing access protocols.	Users need to agree to the terms and conditions before access is approved.	As above	**Low**	Form or other method to capture internal acceptance of the terms and conditions for use of raw data.	**Low**
R-003	Access to raw anonymised data	No established method for users who want raw dataset access bona fide research purposes to request this.	Researchers need to agree to the terms and conditions before access is approved.	As above	**Low**	Need to establish a process for key external stakeholders to request access, how to do this, who reviews and grants access.	**Low**

R-004	Data collection	Using third party contractor, the security of their operating systems, processes and tools.	Procuring services from the third party, they will have access to personally identifying information.	The Contract Service Order outlines the terms and conditions for services procured from RNZ. RNZ meet our security requirements, they satisfied all preconditions of the procurement, their survey tool is SSL certified and they conduct annual penetration testing. RNZ survey platform is General Data Protection Regulation (GDPR) compliant.	**Low**	We will review their next penetration testing results, identifying any gaps. If gaps exists we will co-ordinate additional testing.	**Low**
R-005	Data collection	Access to public servants' personal information (first name and email). Data needs to be well managed.	Data needs to be managed well to ensure that its transferred and stored securely.	Business has an information strategy which covers all information that comes in and out of Te Kawa Mataaho which will be applied to this collection.	**Low**	Use email with SEEMail and in-confidence tags for transferring information and files stored in restricted locations.	**Low**

6. Recommendations to minimise impact on privacy

Ref	Recommendation	Agreed Y/N
R-001	Document the Access, Security and Privacy Protocols for Te Taunaki.	Y
R-002	Establish the terms and conditions for access to raw anonymised data, including method to request access capturing users agreement to terms and conditions.	Y
R-003	Review penetration testing results for all systems RNZ will be using for the census. Apply additional testing where results don't cover all areas which assure us their systems are fully secure.	Y

7. Action plan

This section describes what actions are being taken (whether short or long term) and how they'll be monitored. There may also be links to other processes in the organisation. For example, a proposed action might relate to security controls (such as restricting access to a system). This will then link in with security processes in the organisation.

Reporting on the outcome of the mitigation may be necessary. If the PIA is being performed as part of a project, then the project is likely to require some reporting on their implementation as part of governance arrangements. Once the project is completed, any on-going privacy monitoring should be incorporated into normal business operations.

In the case of a particularly long or complex programme of work, the PIA may need to be reviewed a number of times to ensure that it continues to be relevant. This section should describe how this will be achieved.

Ref	Agreed action	Who is responsible	Completion Date
A-001	Review penetration testing results. If there are any gaps in testing organise and oversee additional testing to take place enabling us to satisfy RNZ systems are fully secure.	IT	
A-002	Draft Access, Security and Privacy Protocols for Census anonymized data - this must include requirement to comply that no publication in a form that could reasonably be expected to identify an individual.	SIT	
A-003	Draft access request form	SIT	
A-004	Document the quality checking process.	SIT	
A-005	Ensure Privacy Statement – accessible to respondents via survey cover requirements outlines in IPP3.	SIT	

Appendix 1: Public Service departments and departmental agencies in scope for the first census

1. Cancer Control Agency
2. Crown Law Office
3. Department of Conservation
4. Department of Corrections
5. Department of Internal Affairs
6. Department of the Prime Minister and Cabinet
7. Education Review Office
8. Government Communications Security Bureau
9. Inland Revenue Department
10. Land Information New Zealand
11. Ministry for Culture and Heritage
12. Ministry for the Environment
13. Ministry for Pacific Peoples
14. Ministry for Primary Industries
15. Ministry for Women
16. Ministry of Business, Innovation and Employment
17. Ministry of Defence
18. Ministry of Education
19. Ministry of Foreign Affairs and Trade
20. Ministry of Health
21. Ministry of Housing and Urban Development
22. Ministry of Justice
23. Ministry of Social Development
24. Ministry of Transport
25. National Emergency Management Agency
26. New Zealand Customs Service
27. New Zealand Security Intelligence Service
28. Oranga Tamariki, Ministry for Children
29. Serious Fraud Office
30. Social Wellbeing Agency
31. Statistics New Zealand
32. Te Arawhiti
33. Te Kāhui Whakamana Rua Tekau mā Iwa – Pike River Recovery Agency
34. Te Kawa Mataaho Public Service Commission
35. Te Puni Kōkiri
36. The Treasury

Appendix 2: Security pre-condition

1.	Provider must be a member of either the Research Association of NZ Inc.; ESOMAR or the Association of Social Science Research.
2.	Provider must hold current professional indemnity insurance.
3.	Track record of delivering products/services of this nature for government, including experience in dealing with large-scale datasets.
4.	Availability of three references from any NZ Government Department should Te Kawa Mataaho wish to consult these.
5.	Provider must be able to demonstrate that they have a fully secure Online Survey Platform/data collection tool. (Completed census responses will upload directly to this Platform and will be accessed only by our contracted research provider.) Ideally the provider will also have a fully certified Portal/File Transfer System: a. for Te Kawa Mataaho to send the master email lists of respondents to the provider and b. for transferring the final dataset back to Te Kawa Mataaho. Provider must be able to provide assurance that the Census Platform and any File Transfer System to be used meets the information security guidelines set out in the New Zealand Information Security Manual (NZISM) v3.3 (https://www.nzism.gcsb.govt.nz/ism-document/)
6.	Provider must be able to provide assurance that they will abide by Te Kawa Mataaho Privacy policy (where applicable) and by the principles under the Privacy Act (including the key changes in the Privacy Act 2020 that will come into effect in December 2020), and that their data security practices will comply with Protective Security Requirements and the EU's General Data Protection Regulation, where this applies.