Public Records Audit Report for the New Zealand Ministry of Foreign Affairs and Trade

Prepared for Archives New Zealand

November 2022

kpmg.com/nz

Disclaimers

Inherent Limitations

This report has been prepared in accordance with our Consultancy Services Order (CSO) with Archives New Zealand dated 26 November 2020. Unless stated otherwise in the CSO, this report is not to be shared with third parties. However, we are aware that you may wish to disclose to central agencies and/or relevant Ministers' offices elements of any report we provide to you under the terms of this engagement. In this event, we will not require central agencies or relevant Ministers' offices to sign any separate waivers.

The services provided under our CSO ('Services') have not been undertaken in accordance with any auditing, review or assurance standards. The term "Audit/Review" used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The information presented in this report is based on that made available to us in the course of our work, publicly available information, and information provided by Archives New Zealand and the New Zealand Ministry of Foreign Affairs and Trade. We have indicated within this report the sources of the information provided. Unless otherwise stated in this report, we have relied upon the truth, accuracy and completeness of any information provided or made available to us in connection with the Services without independently verifying it.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, the New Zealand Ministry of Foreign Affairs and Trade management and personnel consulted as part of the process.

Third Party Reliance

This report is solely for the purpose set out in Section 2 and 3 of this report and for Archives New Zealand and the New Zealand Ministry of Foreign Affairs and Trade's information and is not to be used for any other purpose or copied, distributed or quoted whether in whole or in part to any other party without KPMG's prior written consent. Other than our responsibility to Archives New Zealand, neither KPMG nor any member or employee of KPMG assumes any responsibility, or liability of any kind, to any third party in connection with the provision of this report. Accordingly, any third party choosing to rely on this report does so at their own risk. Additionally, we reserve the right but not the obligation to update our report or to revise the information contained therein because of events and transactions occurring subsequent to the date of this report.

Independence

We are independent of Archives New Zealand in accordance with the independence requirements of the Public Records Act 2005.

Contents

1. Executive summary

The New Zealand Ministry of Foreign Affairs and Trade (the Ministry) represents New Zealand in formal communications with other countries. The Ministry monitors and interprets changes in international political, diplomatic and trade situations to provide the Government with advice and actions to protect and promote New Zealand's interests.

The Ministry implemented SharePoint in 2012 and uses this as the Enterprise Content Management system.

Records are maintained electronically, and physically. Physical records are stored at head office, third party storage providers, and at embassy posts. Due to the classified nature of information, physical records are only accessible by some staff who have appropriate security clearance. Types of records held include trade agreements, international treaties, diplomatic privileges and immunities, funding conditions and arrangements.

The Ministry has approximately 1800 full time staff. The Knowledge, Information and Analytics unit (KIA) has nine full time records management staff that are dedicated to the management of information and data. They are supported by the Data and Information Governance Group which is the Ministry's information management governance group.

The Ministry's information management maturity is summarised below. Further detail on each of the maturity assessments can be found in sections 4 and 5 of this report.

Beginning	**0**
Progressing	**7**
Managing	**9**
Maturing	**4**
Optimising	**0**

2. Introduction

KPMG was commissioned by Archives New Zealand to undertake an independent audit of New Zealand Ministry of Foreign Affairs and Trade (the Ministry) under section 33 of the Public Records Act 2005 (PRA). The audit took place in November 2022.

The Ministry's information management (IM) practices were audited against the PRA and the requirements in the Information and records management standard set out in Archives New Zealand's Information Management Maturity Assessment.

Archives New Zealand provides the framework and specifies the audit plan and areas of focus for auditors. Archives New Zealand also provides administrative support for the auditors as they undertake the independent component of the audit process. The auditors are primarily responsible for the onsite audit, assessing against the standard, and writing the audit report. Archives New Zealand is responsible for following up on the report's recommendations with your organisation.

3. This audit

This audit covers all public records held by the Ministry including both physical and digital information.

The audit involved reviews of selected documentation and interviews with selected staff, including the Executive Sponsor, information management staff, the Information Technology team, and a sample of other staff members from various areas of the Ministry. The Executive Sponsor is the Senior Responsible Officer for the audit.

The audit reviewed the Ministry's information management practices against the PRA and the requirements in the Information management and records standard and provides an assessment of current state maturity. As part of this audit, we completed systems assessments over the Ministry's key systems that act as a repository for public records. This included the document management system, as well as the email and human resource system. Where recommendations have been made, these are intended to strengthen the current state of maturity or to assist with moving to the next level of maturity.

The summary of maturity ratings can be found at Section 4, with detailed findings and recommendations following in Section 5. The Ministry has reviewed the draft report, and a summary of its comments can be found in Section 6.

4. Maturity Assessment

This section lists all assessed maturity levels by topic area in a table format, refer to Appendix 1 for an accessible description of the table. For further context about how each maturity level assessment has been made, refer to the relevant topic area in the report in Section 5.

Category	No.	Topic	Maturity				
			Beginning	Progressing	Managing	Maturing	Optimising
Governance							
	1	IM strategy				●	
	2	IM policy and processes				●	
	3	Governance arrangements & Executive Sponsor				●	
	4	IM integration into business processes			●		
	5	Outsourced functions and collaborative arrangements			●		
	6	Te Tiriti o Waitangi		●			
Self-monitoring							
	7	Self-monitoring			●		
Capability							
	8	Capacity and capability				●	
	9	IM roles and responsibilities			●		
Creation							
	10	Creation and capture of information		●			
	11	High-value / high-risk information		●			
Management							
	12	IM requirements built into technology systems			●		
	13	Integrity of information		●			
	14	Information maintenance and accessibility		●			
	15	Business continuity and recovery		●			
Storage							
	16	Appropriate storage arrangements			●		
Access							
	18	Information access, use and sharing			●		
Disposal							
	20	Current organisation-specific disposal authorities			●		
	21	Implementation of disposal decisions			●		
	22	Transfer to Archives New Zealand		●			

Please note: Topics 17 and 19 in the Information Management Maturity Assessment are applicable to local authorities only and have therefore not been assessed.

5. Audit findings by category and topic

Governance

The management of information is a discipline that needs to be owned from the top down within a public office. The topics covered in the governance category are those that need senior-level vision and support to ensure that government information is managed to ensure effective business outcomes for the public office, our government and New Zealanders.

TOPIC 1 – IM strategy Maturing

Summary of findings

The Ministry has an Internal Content Management and Collaboration Strategy approved by senior management in 2019. It provides strategic direction and supports business needs by assessing and outlining the road map for the future state, as well as the reasons for this direction. The Strategy provides specific guidance and principles for the Ministry's wider Digital Strategy.

The Data and Information Governance Group is the governance group responsible for the information management work programme and ensuring this aligns with the strategy and road map. The Ministry also has regular reporting to the Resources and Organisational Development Committee which is a Senior Leadership Team (SLT) governance committee that also has oversight of information management. Senior leaders across the Ministry actively support the information management strategic direction by setting standards within their teams. For example, senior leaders drive expectations for sending the document link rather than a copy of the document so that only one version of the document is in use at a time.

Senior leaders are aware of the strategy and key points from it are communicated to staff and contractors during the induction. However, there is no refresher training to remind staff and contractors of these key points.

Recommendation

Provide refresher training for staff and contractors to remind them of the intention and key points of the strategy.

TOPIC 2 – IM policy and processes Maturing

Summary of findings

The Ministry has an Information Policy which was approved in March 2022 and aligns with the organisation's strategy. The policy is supported by information management procedures, including disposal, management of information and digitising physical information. These are all located on the business process portal which staff can access from the intranet. All documents on this portal must have a review date attached to it to ensure it remains up-to-date.

Information management job descriptions contain specific information management responsibilities referencing the policy. All other job descriptions include general information management responsibilities. Staff are also required to sign the Code of Conduct which contains some information management responsibilities, such as upholding the integrity of all information on the Ministry's systems. The Code of Conduct was approved in 2013 and is currently going through its first review. The Ministry encourages good information management practice by communicating the importance of the Ministry's information to all staff and promoting good practice through information awareness weeks.

Breaches of the policy can be reported through several channels and are actively addressed through an escalation process. This process means minor breaches can be resolved within the business unit, and larger breaches are escalated to the KIA team to manage.

Information management requirements from the policy are built into all new information systems and business processes that are developed as part of an IT project. This is done through a Data and Information Assessment which is administered by the KIA team and ensures the system or process complies with the Policy. However, information management requirements are not built into new business processes developed outside of an IT project as these are not required to complete a Data and Information Assessment.

Recommendation

Extend the requirement to complete a Data and Information Assessment to all new business processes.

TOPIC 3 – Governance arrangements and Executive Sponsor Maturing

Summary of findings

The Ministry's information management governance group is the Data and Information Governance Group. This is made up of tier three senior leaders and leads the Ministry's data and information vision by championing initiatives and endorsing policies, processes and tools. The Data and Information Governance Group receives regular reporting to understand breaches of the policy and other information management issues.

The Ministry has an SLT committee called the Resources and Organisation Development Committee who support information management. The Committee approves investment, policies and tools and endorses information systems and practices.

The Executive Sponsor consistently fulfils their oversight and monitoring role and has actively promoted the value and importance of information management. The Executive Sponsor acts as the Ministry's main advocate on the SLT and promptly progresses the public release of newly declassified records and seeks to extend resourcing levels. When obligations could conflict with other key business commitments, the Executive Sponsor delegates their responsibilities to appropriate staff (for example, during the Archives New Zealand briefings on the PRA audits). The Ministry will appoint a new Executive Sponsor in December 2022.

The Executive Sponsor does not receive regular reporting but does receive reports when incidents arise. The Executive Sponsor does not currently work with other Executive Sponsors in the sector.

Recommendation

Implement regular reporting to the Executive Sponsor to ensure they remain across current and potential future information management issues.

As appropriate, network with other information management executive sponsors in the sector to discuss information management challenges and opportunities.

TOPIC 4 – IM integration into business processes Managing

Summary of findings

Information management is integrated into all new business processes and activities that are developed as part of an IT project. Business owners must complete a Data and Information Assessment when the business process is created, updated or decommissioned to ensure the business process does not breach any information management responsibilities. The KIA team administers these assessments which ensures information management expertise is included in the business process change and development. However, the Data and Information Assessment is not currently required for new business processes that are developed outside of an IT project. These business processes therefore do not have information management expertise to ensure they comply with information management responsibilities.

The Data and Information Assessment requires business owners to understand their information management responsibilities. However, staff interviewed noted that business owners may not always fulfil their responsibilities as some staff have come from non-government roles and do not always understand the legislative requirements they must comply with.

Recommendation

Provide training and ongoing refresher training to business owners to clarify their responsibilities for managing information within their business unit.

Review the effectiveness of information management processes following the implementation of this training.

TOPIC 5 – Outsourced functions and collaborative arrangements Managing

Summary of findings

The only outsourced contract and collaborative arrangement identified by the Ministry was a contract with another government agency for the administration of scholarships. The Ministry advised us that the contract includes information management requirements, including compliance with the Public Records Act and roles and responsibilities for information management. The Ministry also provides training to the provider to ensure awareness of roles and responsibilities in relation to information management.

There has been no monitoring of the contract as the contract is new. Staff interviewed advised us that monitoring responsibilities sit with the business owner of the contract who will ensure information management responsibilities are met through future compliance audits.

Recommendation

Document a monitoring approach to ensure information management responsibilities in the contract are met.

TOPIC 6 – Te Tiriti of Waitangi — Progressing

Summary of findings

The Ministry is in the early stages of identifying information of importance to Māori and has identified this as a priority. The Ministry intends to appoint a representative for Māori interests to the Data and Information Governance Group to ensure representation at the governance level. The Ministry's Mātauranga group is also working on partnerships with external agencies such as Te Puni Kōkiri to uplift the Ministry's maturity. For example, the Ministry has recently been developing its partnerships in the trade area. The KIA team is also leading the development of a Māori data governance programme, which will provide a draft framework and roadmap to the SLT in February 2023.

The Ministry's process to declassify information has also developed to include a step that assesses whether the information being declassified is of interest to Māori.

Recommendation

Continue to establish processes that will allow the Ministry to locate, identify and use information that is of interest to Māori.

Self-monitoring

Public offices are responsible for measuring and monitoring their information management performance for planning and improvement purposes. This helps to ensure that IM systems and processes are working effectively and efficiently. It also ensures that public offices are meeting the mandatory Information and records management standard as well as their own internal policies and processes.

TOPIC 7 – Self-monitoring

Managing

Summary of findings

The Data and Information Governance Group does not receive regular reporting on the compliance with internal information management policies and processes. However, the Ministry has developed a data assurance plan to implement compliance monitoring. Where issues are identified, the Ministry responds with appropriate actions. For example when some staff were provided unauthorised access to documents, in addition to responding to the specific incident, an email was sent across the organisation explaining the process staff should follow if they find documents they should not have access to.

The Ministry monitors compliance with the Public Records Act through the ComplyWith self-assessment tool. The Audit and Risk Division also conducts audits of the embassies, which includes a physical check of document management practices and a controls survey to ensure staff have the right access levels. However, monitoring and reporting of compliance with information management requirements is not included as part of the Ministry's risk management processes.

Recommendation

Include the monitoring and reporting of compliance with information management requirements as part of the Ministry's risk management processes.

Capability

Information underpins everything our public offices do and impacts all functions and all staff within the public office. Effective management of information requires a breadth of experience and expertise for IM practitioners. Information is a core asset and all staff need to understand how managing information as an asset will make a difference to business outcomes.

TOPIC 8 – Capacity and capability

Maturing

Summary of findings

The Ministry has a dedicated information management team which when fully staffed is considered by the Executive Sponsor and information management staff to be sufficient to meet the Ministry's current and future business needs (excluding the backlog of work to identify, list and appraise its extensive physical information holdings). The Ministry advised that additional capacity and capability will be required to progress the Ministry's maturity, particularly for information architecture and Māori data governance. Information management staff interviewed noted they were often required to do work which was repetitive and time consuming and prevented them from providing advisory support to big projects. For example, locating physical information as the Ministry's system does not allow staff to find physical information and documents easily.

Information management staff have information management responsibilities included in their job descriptions and are measured on these in their performance development plan. Responsibilities are regularly updated to ensure they meet the Ministry's current and future requirements.

Information management staff have access to professional networks as well as related training, such as refresher training on the Public Records Act which was provided by an external facilitator.

Recommendation

Investigate ways to reduce repetitive and time consuming responsibilities of information management staff to enable them to implement continuous improvement in information management practices across the Ministry.

TOPIC 9 – IM roles and responsibilities — Managing

Summary of findings

Information management responsibilities are documented in job descriptions and the Code of Conduct. The Code of Conduct was approved in 2013 and is currently undergoing its first update. Information management responsibilities are promoted through inductions for staff and contractors, and through regular communication. However, the Ministry does not provide regular refresher training beyond these inductions. Good information management practice is embedded into business processes, for example staff must classify the security status of each document as it is created.

The Ministry has a culture of promoting the importance of good information management practice and will regularly monitor whether there is anything that can be done to uplift staff's capability in this area. For example, when a new search function was implemented in the document management system, training was provided to all staff to ensure they were able to use the tool correctly.

Recommendation

Provide regular refresher training for staff and contractors to ensure they understand their information management responsibilities.

Creation

It is important to take a systematic approach to the management of government information, and this starts with an understanding of what information must be created and captured. It is expected that public offices create and capture complete and accurate documentation of the policies, actions and transactions of government. Knowing what information assets are held by public offices is essential to IM practice.

TOPIC 10 – Creation and capture of information **Progressing**

Summary of findings

Based on the focus groups we facilitated, staff and contractors understand and comply with their obligations to create full and accurate records. Information management practices are included as part of induction for all new starters.

Most information is managed in controlled environments to ensure its usability and reliability. For example, staff must use corporate devices for work. As part of the document management system's metadata requirements, a classification must be applied when creating a document to limit access to restricted or confidential information.

Final documents are generally saved in the document management system, but not all documents can be captured due to format or size. Staff interviewed also noted that there are instances of staff incorrectly saving information to their local drive, rather than to the document management system, as some documents could not be located. It was also noted that locating documents on the document management system is difficult due to varying naming conventions.

The KIA team has historically not always been advised or involved in the implementation of new systems and technology that create and capture information. However, recent changes to the project delivery model have strengthened awareness of the requirement to involve information management staff when developing or implementing new systems and services.

Recommendation

Provide ongoing refresher training for staff on the requirements to save Ministry records in records management systems. This should include promoting the importance of creating a record of decisions and business transactions.

Ensure that all new IT systems comply with the Public Records Act and develop a plan to reassess current systems for compliance.

TOPIC 11 – High-value / high-risk information **Progressing**

Summary of findings

The Ministry has an information asset register documenting all information held in digital and physical systems. The Ministry is aware of what high-risk/high-value information is held, but this is not formally identified on the information asset register. This is largely guided by the organisation-specific Disposal Authority.

The Ministry has identified that the process for identifying high-value/high-risk information needs to be formalised, more robust, and explicitly state treatment of such information. The Ministry has contracted an information analyst to formalise the identification process for high-risk/high-value information and will continue this work through 2023.

Recommendation

Assign high-value/high-risk ratings to the information in the information asset register.

Management

Management of information should be designed into systems to ensure its ongoing management and access over time, including following a business disruption event. Information must be reliable, trustworthy and complete and managed to ensure it is easy to find, retrieve and use, as well as protected and secure.

TOPIC 12 – IM requirements built into technology systems — Managing

Summary of findings

Metadata and disposal requirements facilitate the retention of information of long-term value. For example, each information technology (IT) system that stores information has retention rules that automatically identify length of retention.

Information management expertise is involved in the configuration, upgrading and decommissioning of some business systems. The KIA team works with the ICT team and business owner to complete a Data and Information Assessment. Risks relating to business systems that do not meet information management requirements are identified. The KIA team advises the business owner how they can mitigate the risks and the business owner is required to take ownership of actioning this. However, there have been some instances where the ICT team has not involved the KIA team and information management requirements have not been built into the business system (for example, the implementation of new Microsoft technology). Business systems built prior to the implementation of the Data and Information Assessment in 2019 have not been assessed to ensure information management requirements are built into them.

Recommendation

Educate ICT staff and contractors on the obligation to build information management requirements into all business systems.

Develop a plan of work to address business systems built prior to the implementation of the Data and Information Assessment in 2019 to ensure they meet information management requirements.

TOPIC 13 – Integrity of information **Progressing**

Summary of findings

Information management practices are in place to ensure that information is reliable and trustworthy. The document management system has in-built version control, and the Ministry encourages staff to send document links rather than attachments. This is good practice as it encourages people to work on the same document and avoid duplication and misplacement of documents.

A "Smart" search function was implemented six months prior to this audit to assist with document search and retrieval. Staff received training and guidance on how to use this function, but still have variable experiences when trying to find information from the document management system due to inconsistent naming conventions.

There is a general understanding that information created and managed needs to be comprehensive and complete, but no processes are in place to ensure this. For example, the staff we interviewed noted they would often find documents with broken links. Staff also identified that a live tool to check URLs are working would be helpful to provide confidence that the documents created were comprehensive and complete.

Information is inconsistent across the Ministry's different systems. Where inconsistencies are identified, the Ministry assesses and implements appropriate actions. For example, the current work programme has been formed to address inconsistencies with HR information as the Ministry's staff become comfortable with new system processes. Staff identified that it was difficult to know what information was reliable and trustworthy due to this inconsistency. The Ministry does not currently have any plan to assess the integrity of information across all of its systems.

Recommendation

Identify the common issues that staff have in finding and retrieving information and develop a plan to address them.

TOPIC 14 – Information maintenance and accessibility **Progressing**

Summary of findings

The Ministry has a clear security process to manage risks to physical and digital information during business and system changes.

Physical information is stored: on-site; at a facility in Tangimoana; with a third-party provider; and at embassies. Information stored on-site has a location register which shows where the information can be found. There is also access control so only pre-approved people may access the information. Some risks have been identified for physical information and the Ministry is in the early stages of being able to address these.

Preservation and digital continuity needs have been identified for most digital and some physical information, however there are currently no structured plans to address these needs. Action plans to address gaps will be assessed in the upcoming FY23 review.

Technology obsolescence risks are considered for all existing and new technologies. These risks are actively mitigated by the information and technology team.

Recommendation

Implement a plan to address preservation and continuity needs for digital and physical information.

TOPIC 15 – Business continuity and recovery — Progressing

Summary of findings

Business continuity plans (BCP) are owned by various teams and embassies and are specific to the functions of the business unit. The Ministry has identified a need for a consistent, organisation-wide approach, and regular testing. A template is currently in the process of being implemented for embassies to develop their own BCPs and ensure all critical information is identified.

BCP's do not include the salvage and restoration of physical information and this is not regularly tested. The Ministry acknowledges this needs to be improved and is working towards this. For example, in 2021 the Ministry created a physical records standard detailing how public records should be treated so that physical information can be preserved or salvaged. Although digital information is backed up as part of routine IT operational practices, there has not been a recent test of restoration processes for a significant event. This work is being considered for inclusion in the FY23 BCP review.

Recommendation

Continue progressing and implementing consistent BCP templates across all business units and embassies. Ensure BCPs are up to date.

Ensure that the testing of restoration processes is included in the FY23 review.

Storage

Good storage is a very important factor for information protection and security. Appropriate storage arrangements for both physical and digital information ensures information remains accessible and usable for as long as it is required for business and legal purposes and for accountable government.

TOPIC 16 – Appropriate storage arrangements | Managing

Summary of findings

There are appropriate protection and security measures in place to protect physical information against unauthorised access, loss, or destruction at third-party storage providers, and on-site. Digital information must be given a classification and only people with the right permission can access this. Only registered staff are able to access secure physical information and this is monitored by security staff. Staff undergo security training during the induction, relevant to the level of clearance they have, and type of work they are required to do.

Staff interviewed identified that information protection and security risks are sometimes reported to the relevant executive or governance group. Where incidents are identified, these are quickly contained and actions are taken. For example, a staff awareness programme was formed to highlight the importance of physical information after some documents were incorrectly shredded. Another incident involved a staff member accidently deleting a digital folder containing a number of documents. As this incident was resolved within the business unit by recovering the documents from backups, this was not reported to the Data and Information Governance Group. However, all near-misses involving loss, destruction and deletion of information should be reported to the Data and Information Governance Group.

Recommendation

Report on all instances and near-misses of loss, destruction and deletion to the appropriate executive/governance group.

Access

Ongoing access to and use of information enables staff to do their work and the public to hold government accountable. To facilitate this, public offices need mechanisms for finding and using this information efficiently. Information and/or data sharing between public offices and with external organisations should be documented in specific information sharing agreements.

TOPIC 18 – Information access, use and sharing | Managing

Summary of findings

Staff are given information management training at induction, detailing information management roles and responsibilities and how to use the Ministry's tools and systems. Where new tools and systems are introduced, such as the "Smart" search function on the document management system, the Ministry provides training to ensure staff know how to use them. Good information practice is also embedded into ways of working. For example, all Microsoft Office applications have a built-in feature which allows it to connect to the document management system. This makes it easy for staff to save documents in the document management system without having to save it to their desktop first or leave the application.

Access controls for physical and digital information are documented and are in line with legal requirements and business needs. Access controls are monitored and a yearly audit is conducted by KIA to ensure digital access is appropriate for the roles. The document management system and the HR system meets Archives New Zealand's minimum metadata requirements. The Ministry is developing metadata schema as part of the data and information architecture which will be applied to all systems and will enable easier access and sharing of information.

The Ministry has a declassification programme which includes a team of senior staff that proactively declassify records to enable internal staff, contractors and the public to access information.

Information management processes are applied to incoming and outgoing data shared with external parties. This is managed by the legal team, and all contracts with external parties outline information management requirements.

The Ministry does not have visibility over all physical information and the information that is listed is held across multiple spreadsheets and systems. Staff identified challenges accessing physical information and were often required to approach the KIA team to get assistance in locating it.

Recommendation

Perform active maintenance of metadata schema and file plans to ensure the reliability and integrity of information.

Develop a plan to enable greater access, use and sharing of physical information across the Ministry.

Disposal

Disposal activity must be authorised by the Chief Archivist under the Public Records Act. Public offices should have their own specific disposal authority as well as actively use the General Disposal Authorities for disposal of general or more ephemeral information. Disposal should be carried out routinely. Information of archival value, both physical and digital, should be regularly transferred to Archives New Zealand (or have a deferral of transfer) and be determined as either "open access" or "restricted access".

TOPIC 20 – Current organisation-specific disposal authorities Managing

Summary of findings

The Ministry has a current disposal authority which was recently extended until May 2024. Review of the disposal authority is being done by an external contractor to update schedules and ensure it covers all information relating to business functions and formats. This activity was supported by the Data and Information Governance Group.

The Ministry is aware of changes in business and legislative requirements. However, there is no regular review cycle for the disposal authority.

Staff and contractors understand disposal requirements relevant to the information they create and use. Information relating to disposal of physical information is located at printers on each floor of the office building. Staff are instructed to save digital documents onto the document management system once they are finalised and to delete drafts.

Recommendation

Implement a regular review cycle to ensure changes in business or legislative requirements are incorporated into the organisation-specific disposal authority.

TOPIC 21 – Implementation of disposal decisions — Managing

Summary of findings

The Ministry has recently put new processes in place to ensure physical and digital information is retained for as long as required for business use and as identified in authorised disposal authorities. IT systems have retention rules in line with the Ministry and Archives New Zealand requirements, for example ensuring financial records are kept for a minimum of seven years. There is no regular monitoring to ensure disposal processes are efficient in supporting authorised disposal of information.

Disposal actions must be approved by the business owner as per disposal policies. Information management staff are appropriately trained and aware of their disposal requirements and responsibilities. A disposal register is maintained by KIA, and each disposal is endorsed by the relevant business owner. A ‘dispose of records’ document outlines disposal requirements and can be found on the Ministry’s intranet.

The destruction of physical and digital information is secure, complete and irreversible.

Recommendation

Implement ongoing monitoring of disposal processes to ensure they are effective in supporting authorised disposal of information.

TOPIC 22 – Transfer to Archives New Zealand — Progressing

Summary of findings

Physical information of archival value that is over 25 years old, and declassified, has previously been transferred to Archives New Zealand. Prior to information being transferred, it must go through an internal declassification process where it is assessed by a panel. Declassification is based on the sensitivity of the content. If the information is not suitable for declassification, the information will not be transferred to Archives New Zealand and will be reviewed again at a later date.

The Ministry does not currently have a deferral of transfer agreement in place with Archives New Zealand as this expired in 2017. The Ministry approached Archives New Zealand in July 2022 and was advised that for physical records a transfer suspension for the Wellington repository is in place as Archives New Zealand prepares for a move to a new facility.

No digital information has been transferred to Archives New Zealand as the document management system does not have a robust automated function to do this and the Ministry does not have the capability to do so manually. However, a project is underway to replace the current document management system with a system that has an automated function.

Recommendation

Identify digital information of archival value for future transfer to Archives New Zealand.

6. Summary of feedback

The Ministry is thankful for and acknowledges the importance of the Public Records Act audit process and the value generated by Archives New Zealand and KPMG.

The Ministry takes Information Management seriously. We have been driving our records management plan and are pleased that this audit validates our own view that we have made good progress over the last two years.

We will update our records management plan with the audit recommendations and implementation will be monitored by Executive Sponsor with support from our Information Management team and our internal governance processes.

We thank you for the opportunity to review, reflect and readjust, and look forward to achieving our Ministry goal of Maturing.

7. Appendix 1

The table in Section 4, on page 3 lists all assessed maturity levels by topic area in a table format. This table has been listed below for accessibility purposes:

Topic 1, IM strategy – Maturing

Topic 2, IM policy and processes – Maturing

Topic 3, Governance arrangements & Executive Sponsor – Maturing

Topic 4, IM integration into business processes – Managing

Topic 5, Outsourced functions and collaborative arrangements – Managing

Topic 6, Te Tiriti o Waitangi – Progressing

Topic 7, Self-monitoring – Managing

Topic 8, Capability and capacity – Maturing

Topic 9, IM roles and responsibilities – Managing

Topic 10, Creation and capture of information – Progressing

Topic 11, High-value / high-risk information – Progressing

Topic 12, IM requirements built into technology systems – Managing

Topic 13, Integrity of information – Progressing

Topic 14, Information maintenance and accessibility – Progressing

Topic 15, Business continuity and recovery – Progressing

Topic 16, Appropriate storage arrangements – Managing

Topic 18, Information access, use and sharing – Managing

Topic 20, Current organisation-specific disposal authorities – Managing

Topic 21, Implementation of disposal decisions – Managing

Topic 22, Transfer to Archives New Zealand – Progressing

kpmg.com/nz