Public Records Audit Report – Department of Internal Affairs

Prepared for Archives New Zealand

February 2023

kpmg.com/nz

Disclaimers

Inherent Limitations

This report has been prepared in accordance with our Consultancy Services Order with Te Rua Mahara o te Kāwanatanga Archives New Zealand (Archives) 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 and the Department of Internal Affairs. 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 Department of Internal Affairs 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 Section 3 of this report and for Archives and the Department of Internal Affairs 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, 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 in accordance with the independence requirements of the Public Records Act 2005 (PRA).

Contents

1. Executive summary

The role of the Department of Internal Affairs (the Department) is to build a safe, prosperous, and respected nation by connecting our people and communities. The Department has approximately 2,500 full time equivalent staff and has seven branches that cover areas such as Births, Deaths and Marriages, Enterprise Partnerships, and Policy, Regulation, and Communities. The audit does not include the record keeping practises of the Chief Archivist. Section 34 of the PRA requires the Minister to commission an independent audit of the Chief Archivist.

The Department creates or manages records about high value/high risk information including:

- Community development grants and advice, passports, citizenship applications, births, deaths and marriages registrations, charities services, identity verification and document authentication services.
- Heritage collections and taonga, Ministerial and Secretariat Services.
- Ministerial policy advice to the Department s Ministers, regulatory and compliance functions, and monitoring and advice on appointments for several Crown Entities.

This audit primarily focused on the Community Operations Group from Service Delivery and Operations Branch; and the All of Government Services Delivery Group and Agency Partnerships and Capability Group from the Digital Public Service Branch GCPO from the Digital Public Service Branch.

The Department primarily uses an Enterprise Content Management system (ECM) to store its digital records, with many other information systems used by other staff in different functions of the organisation. Physical records are no longer created but legacy physical records are held off site at a secure third party storage provider.

The Information and Data Team has ten roles but at the time of this audit only eight were filled and two were vacant.

The Department 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	**2**
Progressing	**7**
Managing	**9**
Maturing	**1**
Optimising	**1**

2. Introduction

KPMG was commissioned by Te Rua Mahara o te Kāwanatanga Archives New Zealand (Archives) to undertake an independent audit of Department of Internal Affairs under section 33 of the Public Records Act 2005 (PRA). The audit took place in June 2022.

The Department's information management practices were audited against the PRA and the requirements in the Information and records management standard as set out in Archives Information Management Maturity Assessment.

Archives provides the framework and specifies the audit plan and areas of focus for auditors. Archives 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 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 Department including both physical and digital information.

The audit involved reviews of selected documentation, interviews with selected staff, including the Executive Sponsor, Information Management staff, the Information Technology team, and a sample of other staff members from Community Operations Group from the Service Delivery and Operations Branch and All of Government Services Delivery Group; and Agency Partnerships and Capability GCPO from the Digital Public Service branch. Note that the Executive Sponsor is the senior responsible officer for the audit.

The audit reviewed the Department's information management practices against the PRA and the requirements in the Information and records management standards and provides an assessment of current state maturity. 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 Department has reviewed the draft report, and a summary of their 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			●		
	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	●				

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 — Progressing

Summary of findings

The Department does not have an up-to-date Information Management Strategy that provides strategic direction for information management. The last Information Management Strategy was created in 2014 and was approved by senior management at the time. The actions contained in the Strategy had a timeframe of four years from 2014 to 2018.

The 2014 strategy also detailed strategic goals from 2012. Although the Strategy is not up to date, staff interviewed noted that this strategy is still referred to and referenced in planning documents.

The Information and Data Team intends to update the Information Management Strategy this year (22/23 financial year). There is some evidence of planning of a new strategy, shown through the development of a brainstorming document. A three-year Information Management Capability Uplift started in 2021. There is alignment to strategic goals through this project which was supported by Senior Leaders.

Recommendations

Update the Information Management Strategy following Archives guidance. The strategy should support business needs and the current/future strategic direction of the Department.

TOPIC 2 – IM Policy and processes — Managing

Summary of findings

The Department has a current Information Management Policy, which was approved by senior management in March 2022. The Policy includes the roles and responsibilities of staff and contractors within the organisation and is linked to other internal policies at the Department, such as the Code of Conduct and the Privacy Policy. The Policy is consistent with the Archives standard and links to relevant legislation such as the Public Records Act 2005, the Official Information Act 1982, and the Privacy Act 2020.

Generalised department-wide process guidance is available to staff. For example, the guidance material covers processes for saving and deleting information. Information management processes are communicated to staff through mandatory annual refresher training. Staff interviewed said that the policy and processes can be easily accessed through the Department's intranet.

Information management roles and responsibilities are not consistently documented in staff job descriptions. Roles and responsibilities were recorded in two out of the three job descriptions sampled as part of this audit. Some specialist roles (such as Information and Data Team members) have specific role descriptions which cover information management.

Recommendations

Include information management responsibilities in all staff job descriptions.

TOPIC 3 – Governance arrangements and Executive Sponsor — Maturing

Summary of findings

The Department does not have a dedicated information management governance group. The Risk and Assurance Governance Committee (RAGC) undertakes this function. Information management is included in the Terms of Reference for the RAGC and the Executive Sponsor is a member of the group.

The Executive Sponsor actively promotes the value and importance of information management by championing it with senior management and the RAGC. The RAGC is supportive of information management at the Department and gives direction and endorsement for relevant initiatives. For example, the RAGC recently endorsed the annual refresher training.

The Executive Sponsor receives a quarterly Information and Safety Report which includes information management topics. The Safety Report is reviewed at the RAGC and any action or remediation that needs to take place is actioned and followed up by the Executive Leadership Team which the Executive Sponsor is part of

The Executive Sponsor does not actively engage with other Information Management Leaders in the public sector.

Recommendations

The Executive Sponsor should consider engaging with other Information Management Leaders in the public sector on information management.

TOPIC 4 – IM integration into business processes — Managing

Summary of findings

Staff interviewed were aware of their responsibilities for managing information within their branch. The requirements for managing information are contained in the comprehensive guidance process documents created by the Information and Data Team.

Staff noted that managers uphold their information management responsibilities. For example, managers encourage staff to send links via the ECM rather than email file attachments.

Information management expertise is regularly involved in processes and activities at the Department. For example, the Agency Partnership and Capability Team consulted with the Information and Data Team while integrating a new business process. In addition, there are robust processes to support the consideration of information management when developing new or updated business processes. One example is the checklist for onboarding a new Customer Relationship Management (CRM) and ECM system.

Staff from the Information and Data Team noted their intention to establish wider reach and engagement across the Department to ensure they are involved in all business process changes.

Recommendations

Develop, agree, and communicate a process for the Information and Data Team's involvement in business processes and activities across the Department.

TOPIC 5 – Outsourced functions and collaborative arrangements — Progressing

Summary of findings

Requirements for managing information were outlined in all four sampled contracts for outsourced functions. These contracts specify the contracted parties' information management obligations, including creation, management/ownership, retention, and security of information. The Department currently keeps a record of information sharing agreements that capture the purpose and ownership of the information. However, there is no evidence that the Department monitors the information management obligations detailed in these contracts for compliance.

Information management staff are not generally involved in writing or approving information management sections of contracts for outsourced functions or collaborative arrangements. However, a guide for identifying information management requirements was developed to assist staff at the Department when establishing outsourced functions and collaborative agreements. Information staff noted that this guide needed to be re-promoted.

Recommendations

Develop a process to monitor information management requirements in outsourced functions and collaborative arrangements where public records are created and maintained.

TOPIC 6 – Te Tiriti of Waitangi — Beginning

Summary of findings

The Department acknowledges that it holds information of importance to Māori, they had not formally identified what this information is and where within the Department it is held. In addition, there is limited capability within corporate information systems to incorporate metadata in Te Reo Māori. As a result, the Department has not been able to actively improve the accessibility and discoverability of information of importance to Māori.

Recommendations

Identify and assess what information held by the Department is of importance to Māori. This assessment will inform the Department on what further actions are required to address this topic.

Self-monitoring

Public offices are responsible for measuring and monitoring its 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 its own internal policies and processes.

TOPIC 7 – Self-monitoring — Managing

Summary of findings

The Department monitors compliance with the PRA and other relevant legislation through its Annual Legislative Compliance Report. The results of the annual compliance survey are reported along with actions and recommendations for improvements. In 2018/19, an Information Management Uplift programme was established which has committed funding to address actions and recommendations. This programme was replaced by a 3-year Information Management Capability Uplift project, which is a strategic initiative to uplift information management.

The Information and Data Team monitors compliance with the information management policy and its associated processes on an ad-hoc basis. Serious non-compliance is reported to the Executive Sponsor and RAGC through the quarterly Information and Safety Report.

The Information and Data Team periodically reviews personal drives, which are sometimes used to store information (although this is highly discouraged). The Information and Data Team is responsible for approving and monitoring requests for additional storage on these drives. Other monitoring is done over checked-out documents and access control. Self-monitoring results are not currently communicated organisation wide.

Evidence of a structured approach to implement corrective actions to address non-compliance is present. For example, if a staff member sends an email attachment instead of an ECM link, the manager will address this issue with the person. Staff interviewed noted that if they

identified other types of non-compliance, they would let their managers know and were confident that it would be followed up. Through the information management service portal, staff can also request guidance for responding to breaches and non-compliance with the information management policy.

Recommendations

Implement a formal documented process to monitor information management compliance and address issues of non-compliance to ensure a systematic and timely approach.

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 — Progressing

Summary of findings

The Department has a dedicated Information and Data Team made up of eight staff: advisors, senior advisors, a lead advisor, and management. Staff noted in interviews that the current capability and capacity feels appropriate for current organisation needs and that capacity is considered during workflow planning. It was noted during interviews that there is insufficient capacity to routinely carry out disposal decisions (refer to Topic 21 – Implementation of disposal decisions) and to manage the significant changes taking place with Microsoft systems used by the Department.

Capability gaps have been highlighted and work is underway to improve this. For example, there is a plan to fill the current Lead Advisor vacancy and recruit a new coordinator. There has been some disruption following COVID-19 staff movements at the Department. Members of the Information and Data Team have regular access to professional development opportunities such as attending workshops, webinars, and virtual conferences. The team have the necessary capabilities, with most members having information management experience through previous jobs or qualifications.

Recommendations

Ensure IM capacity and capability requirements is regularly assessed and monitored against business needs.

TOPIC 9 – IM roles and responsibilities — Progressing

Summary of findings

Staff interviewed were aware of their information management responsibilities and understood the specific requirements in relation to their role outlined in the Information Management Policy. While responsibilities and requirements are documented for some specialist roles, they are not included in all job descriptions (refer to Topic 2 – IM policy and processes). Some staff members in the focus groups noted that information management is included in their performance plans.

Staff and contractors undergo new starter induction training, mandatory ECM training and sign a Code of Conduct which covers information management. Information management is also covered in the mandatory annual refresher training module. Additionally, it is covered during awareness campaigns, in guidance documents and during additional training (when requested) from the Information Management and Data Team.

Recommendations

Include information management responsibilities in all staff job descriptions, in connection with *Topic 2 – IM policy and processes.*

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 — Managing

Summary of findings

Staff are made aware of their legal obligations to create and capture full and accurate records through new starter induction, on-the-job training, annual refresher training and guidance documents from the Department.

The Department's ECM automatically captures metadata that supports the usability, reliability, and trustworthiness of the information. The ECM meets Archives minimum metadata requirements. As part of this audit, the Grants Management System was also reviewed which has comprehensive metadata functionality built in.

Staff indicated they generally save information in the ECM, which means that information is usable by others and reliable through robust version control, search functionality and audit trails. Staff are discouraged by managers from using personal drives for work purposes, which have limited storage capacity to further discourage use. However, staff noted that information such as drafts are occasionally saved in this uncontrolled environment.

Recommendations

Create and capture information on appropriate systems that meet Archives minimum metadata requirements.

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

Summary of findings

The Information and Data Team has a good understanding of the Department's high-value / high-risk information assets. This understanding is largely guided by the Department's disposal authorities and appraisal reports.

There is an inventory of some information held in digital and physical systems, such as Ministerial documents and Royal Commission inquiries. The Department has trialled an information asset register but does not currently have an active register in place. It was noted during interviews that a review of the high-value / high-risk information assets is in progress.

Recommendations

Create and maintain an inventory of information held in digital and physical systems and identify whether that information is high-value / high-risk.

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

The Information and Data Team and several other branches (such as the Security, Risk and Assurance Team and Information Technology Team) are part of a branch Virtual Team which was set up to provide input into new digital systems. The Virtual Team and the other project teams are routinely involved in consulting on design and configuration decisions relating to most new and upgraded business systems and decommissioning of systems or websites.

A comprehensive checklist/guide (the System Compliance Self-Assessment) was created by the Information and Data Team, which goes through the requirements of the PRA. The Department's project teams Virtual go through the checklist to assess compliance requirements including metadata, and retention and disposal. System design and configuration are also considered during this stage and are documented for business systems.

The primary information management system is the ECM, which meets the minimum metadata requirements. Standardised information management requirements for the ECM are

identified and documented. The ECM allows the Department to incorporate the requirements from the general disposal authorities and organisational-specific authority. However, the Department does not incorporate these documents into the system design.

Recommendations

Integrate and embed the organisation-specific disposal authority into the ECM.

TOPIC 13 – Integrity of information — Managing

Summary of findings

The Department has organisation-wide information practices which are followed by staff. These practices include digitising paper documents, managing text messages and deleting/saving information appropriately. Good practices are encouraged through training and guidance documents. Information practices are in place to ensure information is reliable and trustworthy.

Staff noted that there is variability when finding and retrieving information outside their own branches. However, there are self-help guides and ECM training is available. When completing Official Information Act requests, some staff noted that it is difficult to know whether they have all the information necessary due to the need to obtain information from multiple systems.

Sensitive information in the ECM is classified, and staff who have a need to know, have access to that information. Audit trails are in place, and the minimum metadata, version control and business rules all contribute to the reliability and trustworthiness of information. These mechanisms are actively monitored by the Information and Data Team but there is no regular assessment of whether these controls are functioning correctly.

Recommendations

Identify management controls in place and perform regular testing of these controls to ensure the integrity, accessibility and usability of information is maintained.

TOPIC 14 – Information maintenance and accessibility — Progressing

Summary of findings

Strategies are in place to manage and maintain digital and physical records throughout business and system changes. The Department controls the risks to ongoing accessibility and storage of physical information by managing the information in a third party offsite commercial storage. The Department has location registers for all physical information, and the documents are easily accessible if needed.

During system changes, such as migration or decommissioning, strategies are in place to ensure that digital information remains accessible.

There is a risk of technology obsolescence due to the Department having some records in formats such as audio tapes and backup tapes. The Department is currently developing a plan to address this issue.

Recommendations

Finalise the plan to ensure technology obsolescence risks are identified and mitigated to ensure accessibility.

TOPIC 15 – Business continuity and recovery — Managing

Summary of findings

The Department has Business Continuity Plans (BCP) for each branch. As part of this audit, we looked at a BCP for one of the focus group areas. The BCP was last updated in November 2021, and it identified critical systems and information that would need to be accessed to support business continuity.

The Department undertakes various system back-ups (in several cases these are run daily) which are retained for the length of time deemed necessary.

Information Management staff noted they weren't actively involved in developing or updating BCPs.

Recommendations

Ensure information management expertise is utilised as part of the BCP plans across DIA.

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

The Department has protection and security controls in place for physical and digital information.

Third party storage used by the Department for physical records provides which provides protection against unauthorised access, loss, deletion, or destruction. Information stored offsite is appropriately labelled and easily accessible if required.

Digital information is stored with on-premises systems, on-shore and offshore cloud providers, and appropriate risk assessments were carried out when these arrangements were evaluated. Staff are required to have multifactor authentication on their devices, which is enforced for login when using devices outside the Department's network. Digital information is also protected by access controls and audit logs, although audit logs are not regularly reviewed. There are restrictions on the ability to transmit or store digital records with certain classifications such as 'confidential'.

Information and protection risks are discussed at the RAGC meetings as part of the quarterly reporting. Any risks that are identified are discussed and remediated. However, instances of loss, destruction or deletion are not regularly identified or reported to the RAGC.

Recommendations

Design monitoring and reporting to ensure instances of unauthorised access, destruction or deletion are identified and reported to the RAGC.

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

The Department consistently uses metadata to facilitate the management and discovery of information. The taxonomy embedded in the main ECM enables staff to locate and access records. In addition, comprehensive guidance documents are available to staff for saving and deleting information subject to disposal authorities.

The ECM meets Archives minimum metadata requirements.

Staff and contractors interviewed had a good awareness of the systems and tools they use to capture and access information. Staff noted that there are formal induction processes and regular general information management training. There is no advanced training in the use of metadata and search techniques.

Access controls for information are documented and approved. Specific access is given depending on the role of the staff member or confidentiality of documents. Access controls are regularly monitored and maintained. Staff noted they have sufficient access to carry out their day-to-day jobs. As earlier noted, physical information is kept offsite at a secure third-party storage facility.

Recommendations

Implement advanced training in the use of metadata and search techniques available for all staff and contractors.

Disposal

Disposal activity must be authorised by the Chief Archivist under the Public Records Act. Public offices should have its 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 (or have a deferral of transfer) and be determined as either "open access" or "restricted access".

TOPIC 20 – Current organisation-specific disposal authorities — Optimising

Summary of findings

The Department has current and approved organisation-specific disposal authorities that cover information relating to all business functions. The Department has several disposal authorities which cover all formats and all areas of the organisation.

There is regular review of the disposal authorities, which ensures they reflect business and legislative changes (for example, the changes made to the Privacy Act in 2020). As the Disposal Authorities have a 10-year life cycle, there are also new responsibilities or functions that arise. The Department keeps a register of potential changes or amendments, for example, one amendment in 2019 was approved by the Chief Archivist to address these changes.

Staff interviewed were aware of the disposal authorities and comprehensive guidance documents for disposal were available. Disposal is also covered as part of their yearly information management refresher training.

Recommendations

Due to the assessment of optimising for this topic, we have not made a recommendation.

TOPIC 21 – Implementation of disposal decisions — Progressing

Summary of findings

Disposal actions have been carried out for physical information, but not routinely. Disposals were documented in a disposal register. The last disposal occurred in April 2022 at the third-party off-site facility. Most physical records are held at an offsite storage provider where some records are destroyed on an ad-hoc basis under the disposal authorities. Where the disposal of physical information has occurred, this has been secure, complete, and irreversible.

Disposal of digital information last took place in 2017 when the Department's Shared Workspaces were decommissioned. Most digital record management systems used by the Department do not have the disposal authorities embedded, so regular disposal actions do not take place.

The Department had plans in place to identify resources from the Service Delivery and Operations branch (SDO) and begin appraising records for disposal, however these plans were diverted due to COVID-19.

Recommendations

Implement plan for SDO resources to continue appraising relevant records and disposing when SDO return to normal operations.

TOPIC 22 – Transfer to Archives — Beginning

Summary of findings

The Department has transferred some physical information over 25 years old to Archives. Currently the Department does not have a deferral of transfer with Archives. The Department has not identified digital records over 25 years old.

Physical records held in third-party offsite storage, have not been appraised for information over 25 years old.

Recommendations

Identify physical and digital information that is over 25 years old.

Develop a plan to transfer appropriate digital information to Archives.

6. Summary of feedback

The Department of Internal Affairs is committed to developing and maintaining information management practices that support our daily activities and enable us to meet our business needs, accountability requirements and the expectations of government and the public.

The audit findings have given us a clear sense of where we need to focus over the next 1-5 years to lift our information management maturity. In particular, we need to focus on disposing of the information we are no longer required to keep, and to meeting our obligations under Te Tiriti o Waitangi. We will also be moving from our current enterprise content management system to SharePoint Online. This will provide us with a further opportunity to improve our practices and make it easier to find information.

We look forward to working with Archives New Zealand and other agencies to share knowledge and learn from others' experiences.

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 – Progressing

Topic 2, IM Policy – Managing

Topic 3, Governance arrangements & Executive Sponsor – Maturing

Topic 4, IM integration into business processes – Managing

Topic 5, Outsourced functions and collaborative arrangements – Progressing

Topic 6, Te Tiriti o Waitangi – Beginning

Topic 7, Self-monitoring – Managing

Topic 8, Capability and capacity - Progressing

Topic 9, IM roles and responsibilities - Progressing

Topic 10, Creation and capture of information - Managing

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

Topic 12, IM requirements built into technology systems - Managing

Topic 13, Integrity of information - Managing

Topic 14, Information maintenance and accessibility - Progressing

Topic 15, Business continuity and recovery – Managing

Topic 16, Appropriate storage arrangements – Managing

Topic 18, Information access, use and sharing – Managing

Topic 20, Current organisation-specific disposal authorities – Optimising

Topic 21, Implementation of disposal decisions – Progressing

Topic 22, Transfer to Archives – Beginning

kpmg.com/nz

11 May 2023

Te Rua Mahara o te Kāwanatanga Archives New Zealand
10 Mulgrave Street
Wellington
Phone +64 499 5595
Websites www.archives.govt.nz
www.dia.govt.nz

Paul James
Chief Executive
Te Tari Taiwhenua Department of Internal Affairs Department of Internal Affairs
Paul.james@dia.govt.nz

Tēnā koe Paul

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of Te Tari Taiwhenua Department of Internal Affairs (the Department) completed by KPMG under section 33 of the Public Records Act 2005 (PRA). Thank you for making your staff and resources available to support the audit process.

This did not include an audit of the Chief Archivist's recordkeeping practices, which is separately commissioned by the Minister under section 34.

Introduction

Te Rua Mahara o te Kāwanatanga Archives New Zealand (Archives) is mandated by the PRA to regulate public sector information management (IM). The audit programme is a key regulatory tool in our Monitoring Framework.

Monitoring IM practice across the public sector gives assurance that the government is open, transparent and accountable by providing visibility of public sector IM practices. Full, accurate and accessible information improves business efficiency and government decision-making and accountability, which in turn enhances public trust and confidence. Information that is well managed unlocks the value of government information for the benefit of everyone.

We are confident that you and your organisation are committed to delivering high-quality, trusted information to decision-makers, other government organisations, customers, and stakeholders. We trust that the audit process will support this commitment. The audit report and this letter recommend changes to support improvement of your organisation's IM practices.

Audit findings

In the audit report, the auditor has independently assessed your organisation's information maturity against the framework of our IM Maturity Assessment. Prior to the audit, your organisation completed the Maturity Assessment. This provided a self-assessment of IM maturity for your own use and as context for the auditor about your organisation.

Organisations that are assessed as having a maturity level of 'Managing' across all IM topics are broadly meeting the minimum requirements expected by the PRA and Archives' mandatory Information and records management standard.

The audit report shows the Department with 11 out of 20 topics assessed at 'Managing' or above maturity level. The Department is therefore well placed. There are developments under way that will further enhance this maturity in several topics. These include, for example, the IM strategy update, expanding the reach of the Information and Data Team in business process change, and embedding the disposal authority into the ECM.

Prioritised recommendations

The audit report lists 19 recommendations to improve your organisation's IM maturity.

We endorse all recommendations as appropriate and relevant. To focus your IM improvement programme, we consider that your organisation should prioritise the nine recommendations as identified in the Appendix.

What will happen next

The audit report and this letter will be proactively released on the Archives website shortly. We would be grateful if you would advise of any redactions that your organisation considers are necessary within 10 working days.

As required by the PRA, I will also provide the Minister of Internal Affairs with a report on the results of the audit programme for each financial year, which is tabled in the House of Representatives.

We will follow up this letter with a request to your Executive Sponsor that your organisation provides us with an action plan to address the prioritised recommendations. Our follow up process will track your progress against the action plan.

Thank you again for your support with the audit. In the course of the audit, we have already received feedback from the Department on the application of the IM Maturity Assessment that can inform our future approach to auditing functionally complex organisations. As part of our standard process, we will contact your Executive Sponsor shortly seeking further feedback.

Nāku noa, nā

Anahera Morehu
Chief Archivist
Te Rua Mahara o te Kāwanatanga Archives New Zealand

Cc Darrin Sykes, Deputy Chief Executive Organisational Capability and Services Branch (Executive Sponsor) Darrin.sykes@dia.govt.nz

APPENDIX

Category	Topic Number	Auditor's Recommendation	Archives' Comments
Governance	1: IM Strategy	*Update the Information Management Strategy following Archives guidance. The strategy should support business needs and the current/future strategic direction of the Department.*	It would be useful to update and formalise the strategy informed by the work already done for the Information Management Capability Uplift in 2021.
Governance	5: Outsourced functions and collaborative arrangements	*Develop a process to monitor information management requirements in outsourced functions and collaborative arrangements where public records are created and maintained.*	With increased information sharing and collaboration across the public sector the need for monitoring the requirements for information management will likely increase.
Governance	6: Te Tiriti o Waitangi	*Identify and assess what information held by the Department is of importance to Māori. This assessment will inform the Department on what further actions are required to address this topic.*	The Department creates or works with records of importance to Māori in many of its current and planned activities. An enhanced understanding of these information sources could greatly increase their value.
Capability	8: Capacity and capability	*Ensure IM capacity and capability requirements are regularly assessed and monitored against business needs.*	For a functionally diverse department with many IM systems and processes, the IM team is central in providing specialist advice. The team also needs to monitor and encourage general understanding of IM throughout the organisation. IM work is dynamic as are resourcing needs to support BAU, projects and IM maturity improvement.
Creation	11: High-value/High-risk information	*Create and maintain an inventory of information held in digital and physical systems and identify whether that information is high-value/high-risk.*	This is a very important tool for understanding and prioritising information management across the organisation.

Category	Topic Number	Auditor's Recommendation	Archives' Comments
Management	12: IM requirements built into technology systems	*Integrate and embed the organisation-specific disposal authority into the ECM.*	Automating disposal as much as possible will protect the organisation from over-retention risks.
Management	14: Information maintenance and accessibility	*Finalise the plan to ensure technology obsolescence risks are identified and mitigated to ensure accessibility.*	There is some urgency in addressing risks to information on formats that have a finite life.
Disposal	21: Implementation of disposal decisions	*Implement plan for SDO resources to continue appraising relevant records and disposing when SDO return to normal operation.*	Over retention of information presents risks to the organisation and is an unnecessary cost. Appraisal and disposal of physical records generally should also be included.
Disposal	22: Transfer to Archives	*Identify physical and digital information that is over 25 years old.* *Develop a plan to transfer appropriate digital information to Archives.*	Information that is over 25 years old also needs to be classified as open or restricted prior to transfer. The Department will be aware of the current constraints on physical records transfers. We note that joint work is underway on the transfer of digital records to Archives at the closure of the Royal commission on abuse in care.