Deloitte.

Tumuaki o te Mana Arotake

Office of the Controller and Auditor General

Public Records Act 2005 Audit Report

Prepared for Te Rua Mahara o te Kāwanatanga | Archives New Zealand

Final Report

October 2023

MAKING AN
IMPACT THAT
MATTERS
since 1845

Table of Contents

1. Disclaimers

USE OF REPORT

This report has been prepared in accordance with the Consultancy Services Order dated 1 December 2020 and variation dated 23 September 2021. We have prepared this report solely for Te Rua Mahara o te Kāwanatanga Archives New Zealand (Te Rua Mahara) and the Office of the Controller and Auditor General (the OAG). It was prepared at the direction of Te Rua Mahara and may not include all procedures deemed necessary for the purposes of the reader. The report should be read in conjunction with the disclaimers as set out in the Statement of Responsibility section. We accept or assume no duty, responsibility, or liability to any other party in connection with the report or this engagement, including, without limitation, liability for negligence in relation to the factual findings expressed or implied in this report.

INDEPENDENCE

Deloitte is independent of Te Rua Mahara in accordance with the independence requirements of the Public Records Act 2005. We also adhere to the independence requirements of the New Zealand Auditing and Assurance Standards Board's Professional and Ethical Standard 1 (Revised): Code of Ethics for Assurance Practitioners. Other than this audit programme, we have no relationship with or interests in Te Rua Mahara.

STATEMENT OF RESPONSIBILITY

The procedures that we performed did not constitute an assurance engagement in accordance with New Zealand Standards for Assurance engagements, nor did it represent any form of audit under New Zealand Standards on Auditing, and consequently, no assurance conclusion or audit opinion is provided. The work was performed subject to the following limitations:

This assessment is based on observations and supporting evidence obtained during the review. This report has taken into account the views of the OAG and Te Rua Mahara, and both have reviewed this report.

Because of the inherent limitations of any internal control structure, it is possible that errors or irregularities may occur and not be detected. The procedures were not designed to detect all weaknesses in control procedures as the assessment was performed by interviewing relevant officials and obtaining supporting evidence in line with the guidelines of the Te Rua Mahara Information Management (IM) Maturity Assessment.

The matters raised in this report are only those which came to our attention during the course of performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made. We cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud. Accordingly, management should not rely on our deliverable to identify all weaknesses that may exist in the systems and procedures under examination, or potential instances of non-compliance that may exist.

We have prepared this report solely for the use of Te Rua Mahara and the OAG. The report contains constructive suggestions to improve some practices which we identified in the course of the review using the instructions and procedures defined by Te Rua Mahara. These procedures are designed to identify control weaknesses but cannot be relied upon to identify all weaknesses.

2. Executive Summary

TUMUAKI O TE MANA AROTAKE | OFFICE OF THE CONTROLLER AND AUDITOR GENERAL

Tumuaki o te Mana Arotake | The Office of the Controller and Auditor General (the OAG) is governed by the Public Audit Act 2001 and carries out:

- Annual audits
- Performance audits
- Other assurance services e.g. assurance over information systems, contract management
- Inquiries into issues of concerns.

The OAG is independent of government and serves the purpose of providing Parliament with independent assurance that public organisations are performing and operating in accordance with Parliament's intentions.

In 1992 the Audit Office separated into the OAG and Audit New Zealand (Audit NZ). The OAG became the regulatory body for audits responsible for setting policies and standards, allocating audits, and advising Parliament on the accountability of ministries, departments and agencies. Audit NZ became responsible for providing audit services as allocated by the OAG, thereby enabling the Auditor-General to carry out its function.

In 2006, the OAG and Audit NZ merged their corporate services teams to address resourcing issues. While Audit NZ remains a separate business unit, it is an embedded entity of the OAG and is regarded as in-scope for this audit.

The OAG currently employs 456 full-time employees (FTE) with its head office in Wellington. Audit NZ has regional offices in Hamilton, Auckland, Christchurch, Dunedin, Tauranga and Palmerston North.

A significant amount of information held by the OAG can be identified as being high-value or high-risk including:

- Financial statements of Government
- Performance audit reports and related information
- Significant and/or major inquiries
- Entity assessment, fee mediations, and monthly report reviews
- Management of independence and ethics matters

The Head of Corporate Services at the OAG is the Executive Sponsor (ES) responsible for overseeing IM, who has been in this role since November 2020. The IM team is part of the Information Services Group, which currently has three FTE. The IM Manager reports to the Chief Information Officer (CIO).

SUMMARY OF FINDINGS

We assessed the OAG's IM maturity against the five maturity levels of Te Rua Mahara IM Maturity Assessment model. The results are summarised below:

Maturity Level and Number of Findings

Beginning	2
Progressing	8
Managing	7
Maturing	3
Optimising	-

3. Introduction

BACKGROUND

Te Rua Mahara provides IM leadership across the public sector. This is achieved through monitoring government organisations' IM practices to assure the New Zealand public that:

- Full and accurate records are created and maintained, improving business efficiency, accountability and government decision-making, and in turn, enhancing public trust and confidence in government; and
- Government is open, transparent, and accountable by making public sector IM practices known to the public.

Section 33 of the Public Records Act 2005 (PRA) requires that every public office has an independent audit of its record keeping practices every 5-10 years. The audit programme is part of Te Rua Mahara monitoring and reporting on the state of public sector IM. It is one of the key components of their Monitoring Framework, which also includes a biennial survey of public sector IM and the IM Maturity Assessment.

The Chief Archivist has commissioned Deloitte to undertake these audits of certain public offices and this audit was completed in August 2023.

OBJECTIVE

The objective of the audit is to identify IM strengths and weaknesses within the public office, prioritising areas that need attention and recommending improvements. These audits assist organisations to improve their IM maturity and to work more efficiently and effectively.

SCOPE

Deloitte has undertaken an independent point-in-time assessment of the OAG's IM practices against the IM Maturity Assessment model. The IM Maturity Assessment aligns with the PRA and the standard issued by Te Rua Mahara (the Standard). Topics 17 and 19 of the Te Rua Mahara IM Maturity Assessment are only applicable to local authorities and have therefore been excluded for the purposes of this audit.

The IM Maturity Assessment model classifies the maturity of IM practices from "Beginning" (least mature) to "Optimising" (highest maturity level). The OAG's maturity level for each topic area is highlighted under each of the respective areas. Ratings were based on the OAG's staff responses to questions during in-person interviews and the supporting documents provided pre-audit.

Te Rua Mahara provided Deloitte with the framework including the specified audit plan, areas of focus for the PRA audits, and administrative support to Deloitte. Deloitte completed the onsite audit and audit report, which Te Rua Mahara reviewed before release to the OAG. Te Rua Mahara is responsible for following up on the report's recommendations with the OAG.

Our audit was based on a sample of IM systems, the review of selected documentation on a sample basis, and interviews conducted with a selection of staff in focus groups. As such, this audit does not relate to an Audit as defined under professional assurance standards.

The OAG's feedback to this report is set out in Section 6.

Information Management Maturity Summary

This section lists the Information Management maturity level for each of the assessed topic areas. For further context refer to the relevant topic area in Section 5.

No.	Topic	Beginning	Progressing	Managing	Maturing	Optimising
			Assessed Maturity Level			
		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 Te Rua Mahara	●				

Note: Topics 17 and 19 of the Te Rua Mahara IM Maturity Assessment are only applicable to local authorities and have therefore been excluded.

Audit Findings by Category and Topic

GOVERNANCE

> The management of information is a discipline that needs to be owned 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

High-level statement outlining an organisation's systematic approach to managing information across all operational environments of an organisation.	Maturing

OBSERVATIONS

The OAG has an approved Information Systems Strategic Plan (ISSP). The strategy for IM is integrated into the ISSP, which sets out strategic initiatives for IM through to 2024/25. Key strategic objectives include:

- Investing in systems that support greater insight and improved engagement
- Ensuring critical functions are supported by appropriate technology
- Developing a more secure, resilient, and modern technology environment.

The following seven guiding principles support the delivery of the ISSP:

- Prioritising configuration over customisation
- Managing information as a strategic asset
- Ensuring security and business continuity by design
- Re-using before buying and buying before building
- Integrating solutions
- Considering cloud first
- Favouring tried and tested solutions over cutting edge.

Senior management actively support the ISSP and the strategic direction of IM. The Data, Information, and Technology Governance Committee (DITGC) oversees the progress and implementation of the ISSP. The ES receives direct reporting from the Chief Information Officer (CIO) on the progress of ISSP initiatives. While there is good oversight, there are opportunities to regularly review the strategic direction set out in the ISSP to ensure it is fit-for-purpose.

RECOMMENDATION

Regularly assess the ISSP to ensure objectives are relevant, initiatives are resourced, and outcomes are measurable.

Topic 2: IM Policy and Processes

An information management policy supports the organisation's information management strategy and provides a foundation for information management processes.	Managing

OBSERVATIONS

The OAG has an IM Policy (the Policy), which senior management has approved. The Policy outlines staff members' obligations to create and maintain full and accurate records. This includes the obligation to store records in official systems in a manner which maintains their integrity, security and authenticity.

The Policy is linked to the Te Rua Mahara standard and legislation including the PRA. The OAG recognises the importance of maintaining good IM for transparency and accuracy, and views information as a strategic asset.

Internal policies relating to computer use, copyright and security clearance are also linked to the Policy.

While the Policy has not been updated since December 2015, it is supported by a Protective Security Policy, effective February 2023, which details how the OAG addresses threats and vulnerabilities to information assets.

RECOMMENDATION

Review and update the Policy to ensure it aligns with current business needs.

Topic 3: Governance Arrangements and Executive Sponsor

The Executive Sponsor has strategic and executive responsibility for overseeing the management of information in a public sector organisation.	Managing

OBSERVATIONS

The ES is the Deputy Chair of the DITGC, which is responsible for overseeing the development and implementation of the ISSP as well as identifying and managing data and information system risks. The DITGC has delegated authority from the Combined Leadership Team (CLT) for this purpose and the Chair reports to the CLT after every meeting.

Meeting minutes evidenced updates on the progress of the ISSP, budgeting discussions, and status updates on system projects. Furthermore, the DITGC ensures that managing information aligns with best practice and applicable legislation. While the ES has good oversight of IM activity at OAG there is no direct reporting on IM activity specifically.

Staff interviewed noted that the ES is proactive in championing IM initiatives throughout the organisation. While there is oversight of IM in the organisation, insights can be gained from other organisations in the sector as to current IM practices.

RECOMMENDATION

Ensure updates to the ES incorporate specific IM activities.

Topic 4: IM Integration into Business Processes

All staff should be responsible for the information they create, use, and maintain. Business owners should be responsible for ensuring that the information created by their teams is integrated into business processes and activities. The IM team support business owners and staff.	Managing

OBSERVATIONS

Business owners' responsibilities for IM are outlined in the Policy. Their responsibilities include:

- Understanding the kind of information to be held in the business system
- Ensuring mechanisms are in place to prevent unauthorised deletion of information
- Ensuring that processes are in place to help users create and manage records appropriately.

The IM team reported that issues relating to IM which impact business systems are directed to the appropriate business owner who then consult with IM staff. While responsibilities for business owners are consistently assigned, it was noted that not much is done at the individual level to ensure business owners are fulfilling their responsibilities for IM.

The IM team is involved at the design stage and throughout the development of processes to ensure IM is appropriately integrated and to avoid future issues.

RECOMMENDATION

Ensure business owners actively fulfil their responsibilities for managing information within their business unit.

Topic 5: Outsourced Functions and Collaborative Arrangements

Outsourcing a business function or activity or establishing collaborative initiatives does not lessen an organisation's responsibility to ensure that all requirements for the management of information are met.	Progressing

OBSERVATIONS

The OAG has a range of service-level agreements with third-party vendors. These contracts are subject to a range of requirements outlined by the Procurement Team. These requirements cover responsibilities for IM and specifically address usability and accessibility, security, and compliance. Moreover, the requirements specify that service-level agreements are to align with PRA obligations.

Contractors are required to sign the code of conduct, computer use requirements, and confidentiality agreements. Outside of this, risks of non-compliance are not monitored. IM staff advised that compliance with contracts is largely based on trust.

RECOMMENDATION

Identify and address the risks of non-compliance by any party involved in outsourced functions and collaborative arrangements.

Topic 6: Te Tiriti o Waitangi

The Public Records Act 2005 and the information and records management standard supports the rights of Māori under Te Tiriti o Waitangi/Treaty of Waitangi to access, use and reuse information that is important to Māori.	Beginning

OBSERVATIONS

The OAG has not identified information of importance to Māori. There are plans in place to implement a te ao Māori strategy aimed at developing understanding of Te Tiriti o Waitangi and te reo Māori capabilities within the OAG.

RECOMMENDATION

Identify and document information of significance to Māori in an Information Asset Register (IAR).

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 internal policies and processes.

Topic 7: Self-Monitoring

Organisations should monitor all aspects of their information management.	Progressing

OBSERVATIONS

The OAG conducts a certification and accreditation process (C&A) for all new systems, thereby monitoring compliance with the PRA and other relevant legislation. Systems are subject to the C&A process on a three-year cycle. A third party legislative compliance monitoring tool is also used, and results are reported annually to the CLT.

The OAG's ICT security framework supports the development of internal monitoring of IM policies and processes. This will involve a maturity assessment and dashboard reporting on IM.

RECOMMENDATION

Complete the development of regular monitoring of internal IM policies and processes and reporting to DITGC.

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

Organisations should have IM staff or access to appropriate expertise to support their IM programme.	Progressing

OBSERVATIONS

There is a budget for professional development for the IM team. Staff interviewed reported that the IM team are highly competent and capable, and sought out for advice. IM staff, however, stated that capacity proves to be an issue. The IM Manager indicated that capacity and resourcing will likely become an issue as the ISSP progresses.

The ES stated that while they consider capacity was currently sufficient, there would likely be a need to address resourcing in the future. The ES noted that some mapping of future resource needs has been completed particularly for migrations and system upgrades as set out in the ISSP.

RECOMMENDATION

Ensure IM capacity is regularly assessed and appropriately resourced to address business needs.

Topic 9: IM Roles and Responsibilities

Staff and contractors should be aware of their responsibility to manage information.	Progressing

OBSERVATIONS

New staff at the OAG undertake induction training where the Policy, practices, and processes are discussed. There is also training for staff on relevant business systems and tools. Refresher training is provided on request and IM modules are available to staff, although not compulsory. Staff advised they are ultimately responsible for their own training, with the IM team educating and providing guidance when requested.

IM roles and responsibilities are largely well understood by staff, with roles and responsibilities only communicated through the Policy and related guidelines.

RECOMMENDATION

Assess the need for ongoing IM training and plan to address any identified need.

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

Every public office and local authority must create and maintain full and accurate information documenting its activities.	Managing

OBSERVATIONS

The primary Electronic Document Management System (EDMS) used at the OAG is Source, a SharePoint 2016 based system. Source is used for the storage of corporate information including information relating to core services of the OAG such as audit reports, reports to Parliament and performance audits. The primary system for Audit NZ is TeamMate and includes audit working papers and entity related information. The Audit Status Database (ASD) is another key system the OAG uses to manage audit contracts, audit returns and associated documentation.

These systems are all either planned to be, or in the process of being replaced. As outlined in the ISSP, Source is currently being migrated to SharePoint Online, TeamMate is to be replaced by Auviner (SharePoint solution), and ASD with a new contract management and self-service portal.

The use of personal systems as well as non-approved cloud systems is prohibited.

Interviews indicated that staff have a strong understanding of their responsibilities to create and capture information. Staff are also prompted to add metadata to information being stored in Source. While Source requires some metadata to be entered, staff advised that additional metadata is also entered as a matter of good practice.

Staff expressed confidence regarding their ability to capture full and accurate records, however, some barriers to this were identified. Some staff advised that they have difficulty entering metadata into Source as they are not sure of its purpose or if they are entering it correctly.

Moreover, some staff noted that the effort required to enter information into Source also forms a barrier. This is due to documents needing to be saved to the desktop before being uploaded and then entering metadata.

RECOMMENDATION

Address the useability issues in the set-up of the new EDMS.

Topic 11: High-Value/High-Risk Information

Staff and contractors should be aware of their responsibility to manage information. Every public office and local authority must create and maintain full and accurate information documenting its activities.	Progressing

OBSERVATIONS

The OAG does not currently have an IAR formally identifying information of high-value/high-risk. There is some identifying of the value and risks to information held in certain systems, however, this is generally for a purpose such as evaluating information prior to a migration.

RECOMMENDATION

Formally identify high-value/high-risk information assets in an IAR.

MANAGEMENT

Management of information should be designed into systems to ensure its ongoing management and access over time, including following a business disruption event. The 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 Solutions

IM requirements must be identified, designed, and integrated into all of your organisation's business systems.	Maturing

OBSERVATIONS

IM requirements are considered when configuring new systems and decommissioning of technology systems. This is largely through the C&A process in which PRA requirements are embedded. PRA requirements are also included in the OAG's non-functional requirements which are used when procuring systems. Disposal processes and metadata are built into key systems. As well as this, exit strategies are identified through the C&A process to facilitate the retention of information of long-term value.

There was a recent decommissioning of a database, which the IM team were involved in. The decommissioning involved documenting what information was being moved and where to.

IT staff also reported that IM is considered throughout a systems lifecycle, including preparing for systems' exits by building considerations into agreements at the start. Regarding system changes, IT staff noted that user acceptance testing, among other tests, are conducted to ensure the integrity of information following a migration. Documentation is available for all systems and is updated when a system undergoes a change.

Te Rua Mahara minimum metadata requirements are met in all in-scope systems.

RECOMMENDATION

Ensure disposal requirements and processes are fully built into all new and upgraded technology systems.

Topic 13: Integrity of Information

Information should be managed so that it is easy to find, retrieve and use, while also being secure and tamper-proof.	Progressing

OBSERVATIONS

Staff were confident in their ability to create complete and comprehensive records. Version control is built into key repositories such as Source and TeamMate, however it was reported that naming conventions are more consistent in TeamMate (which Audit NZ primarily uses) than in Source (which OAG primarily uses).

Lack of naming conventions in Source, as well as other findability issues (see Topic 18) mean staff have variable experiences when trying to find and retrieve the information they need.

The IM team advised that due to system limitations, there is little that can be done to improve taxonomy in Source outside of the planned migration to SharePoint Online.

RECOMMENDATION

Assess issues with findability of information such as naming conventions and taxonomy and ensure these are addressed in the new EDMS.

Topic 14: Information Maintenance and Accessibility

Information maintenance and accessibility cover strategies and processes that support the ongoing management and access to information over time.	Progressing

OBSERVATIONS

All of the OAG's significant information in physical format is accessed from, and maintained by, their third-party storage provider.

There are strategies in place to manage and maintain digital information during business and system changes. This largely involves gaining an understanding of the scope of information that needs to be migrated. Records no longer described as active records have a formalised trigger to go through the retention and disposal process.

Strategies for the long-term preservation of digital information have not yet been formally identified.

RECOMMENDATION

Identify and formally document a digital continuity strategy

Topic 15: Business Continuity and Recovery

This covers the capability of the organisation to continue delivery of products or services, or recover the information needed to deliver products or services, at acceptable pre-defined levels following a business disruption event.	Managing

OBSERVATIONS

While the OAG has an organisation-wide business continuity management policy. It could not be sighted by the auditors due to issues of confidentiality.

Business continuity plans are managed by the CISRO and reviewed annually by the CLT. There are also quarterly assessments to ensure alignment with other independent programmes within the OAG.

The OAG has a set of disaster recovery procedures which outline recovery time objectives and recovery point objectives for systems. Critical systems are protected by a third-party which also provides regular backup testing. The last backup test was conducted in November 2022 and did not identify any issues.

The IM Manager was involved in establishing the disaster recovery procedures and was consulted with for the prioritisation of systems. The IM team also have a strong understanding of their roles in a business disruption event.

RECOMMENDATION

Consider consulting expertise for the salvage and restoration of physical business information

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

Appropriate storage arrangements for both physical and digital information ensures information remains accessible and usable throughout its life.	Maturing

OBSERVATIONS

As stated above, all significant information in physical format is held at a third-party storage provider.

The majority of digital information is held onshore. Information held oversees is kept in countries party to the Five Eyes alliance. The GCDO cloud risk assessment is completed for every new cloud-based solution. A range of mechanisms are employed to protect information from unauthorised access or loss including access controls, firewalls, and third-party cyber security monitoring.

The C&A process also plays a key role in ensuring secure storage with providers. Risks identified are reviewed by the certification body which is comprised of the Controller and Auditor-General, Assistant Auditor General (AAG) Corporate Services, AAG-Legal, the Chief Information Security and Risk Officer (CISRO), and the Chief Information Officer. Risks are discussed with relevant business owners and only accepted if they have a clear path to mitigation.

There is also a process for investigating security risks, which the IM team undertakes and escalates issues as necessary to the CISRO. Incidents are categorised as either a breach or a near miss. The review process requires all incidents to be reported. Privacy incidents are to be reported to the Privacy Officer, AAG-Legal, Policy, and Inquiries, while security incidents are reported to the IM Manager.

The IM team stated that they are confident that digital information held both onshore and overseas is secure.

RECOMMENDATION

Establish regular monitoring of remediation actions.

ACCESS

> Ongoing access to and use of information enables staff to do their jobs. To facilitate this, organisations will need mechanisms to support the findability and usability of information. Information and data that is shared between organisations is identified and managed.

Topic 18: Information Access, Use and Sharing

Staff and contractors are able to easily find and access the information they need to do their work. Access controls for information is documented and consistently applied and managed. Metadata facilitates discovery and use of information. Information and data received or shared under information sharing agreements is managed according to IM policies and processes.	Progressing

OBSERVATIONS

Staff interviewed largely reported that they have the appropriate access permissions to carry out their work. There are instances where staff have found that they do not have sufficient access for their roles, although it was reported that the processes in place to request permissions work efficiently. Staff looking to request further permissions go through an approval process with the relevant business owner or an automated ticket, which the IM team manages.

IT staff stated that reviews occur daily to ensure permissions are applied correctly and that access requests are automated wherever possible. There were no instances of having too much access reported.

For external information sharing, there are formal sharing agreements and protocols. These outline the obligations of both parties to maintain confidentiality and security.

Internally, staff reported that finding the information they need to do their work is difficult. This issue mainly relates to Source, which is due to the poor search functionality resulting in the need to apply metadata to bypass this issue. While there is a metadata schema in place, it is inconsistently applied by staff.

IM staff reported that addressing these findability issues should be a key consideration when migrating to SharePoint Online.

RECOMMENDATION

Improve search functionality and ensure a consistent metadata schema in the new EDMS to facilitate efficient management and discovery of information.

DISPOSAL

> Disposal activity must be authorised by the Chief Archivist under the PRA. 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 (or have a deferral of transfer) and be determined as either "open access   or "restricted access".

Topic 20: Current Organisation-Specific Disposal Authorities

This is about an organisation having its own specific disposal authority, not the implementation of the disposal actions authorised by the authority. It is not about the General Disposal Authorities.	Managing

OBSERVATIONS

The OAG has a current and approved Disposal Authority (DA). The DA covers all information formats and business functions. It was approved in February 2020 and was last reviewed in December 2022. This review was to ensure the retention and disposal schedule was fit for purpose regarding cloud-based document management.

No significant barriers were identified regarding staff disposing of information. However, staff advised it is sometimes unclear on the disposal requirements, therefore they generally employ a risk averse approach.

RECOMMENDATION

Ensure staff and contractors understand the disposal requirements relevant to the information they create and use.

Topic 21: Implementation of Disposal Decisions

This is about the implementation of disposal decisions, whether from organisation-specific disposal authorities or the General Disposal Authorities.	Managing

OBSERVATIONS

Information is disposed of in accordance with the OAG's DA and General Disposal Authorities (GDAs). The relevant business owner must approve of the disposal before the IM Manager endorses and the ES approves.

Qualitative testing is conducted to ensure the disposal of digital information is complete. Disposal of physical information is handled by the third-party storage provider following sign-off from the relevant business owner.

Information is disposed of approximately every two years, and this is documented in a disposal register. The process for disposal is documented and sets out key steps and considerations. Retention and disposal actions are carried out across some repositories.

RECOMMENDATION

Ensure the retention and disposal schedule is applied to all new business systems planned in the ISSP.

Topic 22: Transfer to Te Rua Mahara

Information of archival value, both physical or digital, should be regularly transferred to Te Rua Mahara or a deferral of transfer should be put in place.	Beginning

OBSERVATIONS

Physical and digital information of archival value that is over 25 years old has not been identified. The OAG also has not engaged with Te Rua Mahara to plan or defer transferring of information.

RECOMMENDATION

Identify and document all physical and digital information of archival value that is over 25 years old.

Summary of Feedback

The Office of the Controller and Auditor-General ("the Office") has reviewed the outcomes and recommendations of the recent Public Records Act audit conducted by Archives NZ. We consider that this audit report is a fair, factual, and accurate picture of the Office's information management practices and capabilities.

We have identified actions that the Office will take as a consequence of the review. These actions will lift and promote our ongoing information management maturity and capability across the Office.

The action plan will be overseen by our Executive Sponsor and Governance Committee, which ensures the Office's information remains a valued, well managed, and business-aligned strategic asset.

Deloitte.

23/11/2023

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

John Ryan
Controller and Auditor General
The Office of the Controller and Auditor General
john.ryan@oag.parliament.nz

E te rangatira e John, tēnā koe

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of Tumuaki o te Mana Arotake Office of the Controller and Auditor General (the OAG) completed by Deloitte under section 33 of the Public Records Act 2005 (PRA). Thank you for making your staff and resources available to support the audit process.

Introduction

Te Rua Mahara o te Kāwanatanga Archives New Zealand (Te Rua Mahara) 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 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.

Kia pono ai te rua Mahara – Enabling trusted government information

Auckland Regional Office, 95 Richard Pearse Drive, Mangere, Auckland
Christchurch Regional Office, 15 Harvard Avenue, Wigram, Christchurch
Dunedin Regional Office, 556 George Street, Dunedin

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 the mandatory Information and records management standard. The OAG's IM maturity is assessed as mostly at 'Progressing' level and above with three topics at 'Maturing'. This is a good basis to develop from and the audit report Summary of Feedback section from your organisation indicates that actions for improvement have already been identified.

Prioritised recommendations

The audit report lists 20 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 eight recommendations as identified in the Appendix.

What will happen next

The audit report and this letter will be proactively released on our 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. We would greatly appreciate further feedback on the audit process and the value it provides to organisations. We have sent a feedback survey link for the attention of your Executive Sponsor in the accompanying email.

Nāku iti noa, nā

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

Cc Becky MacNeill, Assistant Auditor General, Corporate Services (Executive Sponsor), Becky.MacNeill@oag.parliament.nz

APPENDIX

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Governance	2: IM Policy and Processes	*Review and update the Policy to ensure it aligns with current business needs.*	The IM Policy is a foundational document setting the OAG's expectations for the organisation's IM and should be up-to-date and relevant.
Governance	5: Outsourced Functions and Collaborative Arrangements	*Identify and address the risks of non-compliance by any party involved in outsourced functions and collaborative arrangements.*	Understanding the risks will help the organisation target which contracts should be monitored for their IM.
Governance	6: Te Tiriti o Waitangi	*Identify and document information of significance to Māori in an Information Asset Register (IAR).*	This is a topic that generally needs uplift across most public offices and the OAG may benefit from working on this with other similar organisations.
Self-Monitoring	7: Self-Monitoring	*Complete the development of regular monitoring of internal IM policies and processes and reporting to DITGC.*	Agreeing on what will be monitored and reporting on that to the DITGC through the Executive Sponsor would be useful in raising visibility of IM issues and trends.
Capability	8: Capacity and Capability	*Ensure IM capacity is regularly assessed and appropriately resourced to address business needs.*	This includes the IM initiatives in the ISSP as well as BAU.
Creation	11: High-Value/High-Risk Information	*Formally identify high-value/high-risk information assets in an IAR.*	This work will help the organisation prioritise its IM effort concentrating on high-value/high-risk information assets.

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Management	13: Integrity of Information	*Assess issues with findability of information such as naming conventions and taxonomy and ensure these are addressed in the new EDMS.*	The design and configuration of the new EDMS needs the involvement of IM expertise to ensure that it supports the management of information and improves the user experience. This will also address the recommendation for Topic 18: *Information Access, Use and Sharing*.
Management	22: Transfer to Te Rua Mahara	*Identify and document all physical and digital information of archival value that is over 25 years old.*	This will assist the OAG realise the benefit of their current DA and will inform discussion with Te Rua Mahara around transfer.