Deloitte.

Office of the Ombudsman | Tari o te Kaitiaki Mana Tangata Public Records Act 2005 Audit Report

Prepared for Archives New Zealand

April 2022

MAKING AN IMPACT THAT MATTERS since 1845

Table of Contents

1. Disclaimers

Use of Report

This report was prepared for the use of Archives New Zealand (Archives NZ) and Office of the Ombudsman. It was prepared at the direction of Archives NZ 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 Archives NZ in accordance with the independence requirements of the Public Records Act 2005. We also adhere to the independence requirements of Professional and Ethical Standard 1 (Revised): Code of Ethics for Assurance Practitioners issued by the New Zealand Auditing and Assurance Standards Board. Other than this audit programme, we have no relationship with or interests in Archives NZ.

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 Office of the Ombudsman and Archives NZ who 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 Archives NZ's 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 Office of the Ombudsman and Archives NZ. 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 Archives NZ. These procedures are designed to identify control weaknesses but cannot be relied upon to identify all weaknesses.

2. Executive Summary

Office of the Ombudsman

The Office of the Ombudsman (the Ombudsman) is an Office of Parliament, established in 1962 and governed by the Ombudsman Act 1975. The Ombudsman's overall purpose is to investigate, review, and inspect conduct and decision-making and provide advice and guidance to ensure people are treated fairly.

At the time of this audit the Ombudsman has 170 staff based in Wellington and Auckland and have expanded substantially in recent years. The main business groups are Corporate Services, Complaints Resolution, Systemic and Monitoring, Strategy, Engagement and Development, Legal and Finance.

Information of high-risk / high-value includes casework concerning individual complaints and proactive, self-initiated investigations into possible systemic issues, deaths in custody, inspection and evidence records for examining both public and private places of detention, advice and guidance to agencies, Ministers and whistleblowers, disability convention monitoring, practice guidelines and corporate management.

The Ombudsman has an Information and Knowledge Management team (IKM) comprising of four FTEs, which provide IM services to the organisation and action IM parts of the Information Systems Strategic Plan (ISSP).

Summary of Findings

We assessed the Ombudsman's IM maturity against the five maturity levels of Archives NZ's IM Maturity Assessment model. The results are summarised below:

Maturity Level	Beginning	Progressing	Managing	Maturing	Optimising
No. of Findings	2	5	10	2	1

3. Introduction

Background

Archives NZ 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;
- 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 Archives NZ's monitoring of and reporting on the state of public sector IM. It is one of the key components of their Monitoring Framework, which also includes an annual survey of public sector IM and the IM Maturity Assessment.

The Chief Archivist has commissioned Deloitte to undertake these audits for certain public offices.

Objective

The objective of these audits is to identify areas of IM strengths and weaknesses within the public office, prioritising areas that need attention and what needs to be done to strengthen them. They are seen as an important mechanism for 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 Ombudsman's IM practices against Archives NZ's IM Maturity Assessment Model. The IM Maturity Assessment aligns with the PRA and Archives NZ's mandatory Information and Records Management standard. Topics 17 and 19 of the Archives NZ 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 Ombudsman's maturity level for each topic area is highlighted under each of the respective areas. Ratings were based on the Ombudsman's officials' responses to questions during online interviews and the supporting documents provided in line with the IM Maturity Assessment guidelines.

Archives NZ 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 Archives NZ reviewed before release to the Ombudsman. Archives NZ is responsible for following up on the report's recommendations with the Ombudsman.

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 and focus groups. As such, this audit does not relate to an Audit as defined under professional assurance standards.

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

4. 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.

Category	No.	Topic	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 Archives New Zealand		●			

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

5. 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 Ombudsman has a current IM strategy, the Information Services Strategic Plan (ISSP), which the Senior Management Team (SMT) and the Board have approved. The ISSP sets out the strategic direction for the Information and Knowledge Management team (IKM) and Information Communications Technology team (ICT). It identifies key IKM initiatives for 2021-2024. Due to frequent changes in technology, and to ensure relevancy to the Ombudsman's broader strategic direction, the ISSP is reviewed at least annually. Its progress is a standing item on monthly Information Management Policy and Strategy Governance Group (IMPSG) meetings. The IKM Manager also provides regular reports to the Executive Sponsor (ES) on the ISSP work programme.

The content of the ISSP covers the constitutional context of the Ombudsman, its work relating to the Te Tiriti o Waitangi as an independent Office of Parliament, purpose, principles, enabling capabilities, strategic themes, and the ICT and IKM priority work programmes.

The ISSP is part of the organisational strategic planning framework and is informed by the Ombudsman's purpose and strategic direction. The ES is the ISSP owner and it is available on Waka, an enterprise content management system.

Recommendation

1. Ensure the ISSP is reviewed annually, in July, and updated with any relevant business initiatives.

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 Ombudsman has an approved IM policy (the Policy), which is currently under review. The Policy includes roles and responsibilities for both general staff and IKM specialists, an Information and Records Management Framework, principles, policy statements and all relevant legislation. The Policy, along with the ISSP, is available on Waka.

The Policy is a foundational document, which is supported by several IM guides and process documents.

Recommendation

1. Review and update the Policy, as planned, including adding when due for next review.

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.

Maturing

Observations

The Ombudsman has an Information Management Policy and Strategy Group (IMPSG), a formalised governance group with its own Terms of References, which is regularly reviewed. The monthly IMPSG meeting minutes record the key recommendations for the SMT on IKM and ICT initiatives and receives a regular monthly report from the Manager IKM. Members of IMPSG include Manager IKM, Manager ICT, Manager People and Capability, Manager Communications, Chief Financial Officer, Deputy Ombudsman, Senior Assistant Ombudsman Strategy, Engagement and Development, Assistant Ombudsman Systemic and Monitoring, Assistant Ombudsman Complaints Resolution, Chief Legal Officer, Virtual Chief Information Officer, and the Chief Ombudsman. The ES, the Assistant Ombudsman, Corporate Services, chairs the IMPSG.

Feedback consistently indicated that the ES is a critical leader for IM at the Ombudsman. This is shown through a significant involvement in IMPSG, a mature ISSP and Policy, which has the support of the SMT and the Board. The ES actively promotes the value of IM and continues to support the work programme to ensure IM is integrated into all facets of the business. Improving the Ombudsman strategic IM programme could be achieved by sharing, both ways, good practice with other ES's in the sector.

Recommendation

1. The ES to develop connections with other ES to gain experience and share good practice.

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

Staff generally understand and consistently fulfil their responsibilities for managing the information they create, use, and maintain, particularly relating to investigation case files. Investigators have rigorous training on case management including IM practices, due to the nature of the role. There are also quality assurance checks at case closure, which promotes good practice recordkeeping.

All staff undertake mandatory IM induction training, which includes reviewing the Policy that outlines business owners' roles and responsibilities.

IKM functions as an IM services team to provide support on IM practices, use of the Ombudsman's recordkeeping systems, and IM guidance on Awa. Staff reported having a general understanding of IM and knew where to find IM expertise if they require any support. However, several were not aware of IM resources available on Awa or that the IKM team has a high-level of technical knowledge on IM practices.

Recommendation

1. IKM to assess business owners needs to ensure they actively fulfil their IM roles and responsibilities 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 Ombudsman is an independent Office of Parliament with statutory secrecy and confidentiality requirements and is unable to enter into shared agreements with Crown Entities and government agencies. Under s160 of the Corrections Act 2004 the Ombudsman has signed a statutory protocol with Ara Poutama Aotearoa |Department of Corrections,

which enables read-only access to its Integrated Offender Management System (IOMS) for limited reasons. A review of this agreement showed very limited reference to IM roles and responsibilities, with a minor reference to the PRA through compliance with relevant legislation.

The Ombudsman has service contracts, including with its primary IT service provider. Whilst none create public records, they all referenced confidentially, security, storage of information, privacy, and intellectual property. Compliance with all New Zealand law was the only reference to the PRA.

There is no regular monitoring over the contracts in place to ensure compliance with the PRA.

Recommendation

1. Ensure relevant IM requirements are included in all contracts where public records are created and develop a regular monitoring process to ensure suppliers are compliant with IM requirements under the PRA.

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

Information of importance to Māori has not yet been identified. Currently demographic information is not collected for every complainant therefore it is difficult to proactively identify information specific to Māori, However, annual awareness surveys are conducted, which cover ethnicity and informs planning and engagement activities.

The Ombudsman has developed a te ao Māori transformation programme of work which aims to ensure the Ombudsman's practices are consistent with the Treaty and its principles. They have established a panel of eminent Māori rangatira to advise and a new Ombudsman team, Rōpu Māori Hononga Hapori to advise on this.

This te ao Māori transformation plan includes gaining guidance to develop the Chief Ombudsman's recognition of Te Tiriti o Waitangi statement within the ISSP. A data management strategy is also being developed and work has already started on exploring Māori data sovereignty.

The Ombudsman is replacing the current case management system with a new application that will have updated metadata requirements. This will assist with identifying information specific to Māori and may incorporate Te Tiriti o Waitangi requirements into the metadata.

Recommendation

1. Work with Rōpu Māori Hononga Hapori to incorporate Te Tiriti o Waitangi and align the Ombudsman's te ao Māori transformation work programme into the ISSP and IKM work programmes, specifically to identify information of importance of 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 internal policies and processes.

Topic 7: Self-Monitoring

Organisations should monitor all aspects of their information management.

Managing

Observations

The Ombudsman completes an annual ComplyWith survey, a legislative compliance tool. The survey report identifies areas of non-compliance and SMT monitors actions through to resolution. Previous ComplyWith reports show any risks to non-compliance with the PRA have been reported and mitigating actions taken.

Additionally, within the Complaints Resolution Group, which focuses on investigations, a Quality Assurance Framework is applied at case closure where any recordkeeping issues are identified and remedied.

There is currently limited monitoring over third-party contracts and sharing agreements.

Recommendation

1. Develop a work programme activity to actively monitor compliance with the IM Policy across business units.

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.

Optimising

Observations

The Ombudsman's IKM team comprises a full time IM manager, one senior IM advisor, one senior ECM advisor, one senior data analyst, and a seconded one-year data analyst. Staff members tend to have specialities in one or more of the core systems. The work programme consists of a roadmap to achieve the ISSP objectives, along with the ICT team. The current team has sufficient skills and capacity to achieve the work programme and provide expertise across a multitude of areas.

IKM has access to broader professional development opportunities to support the organisation's direction and their own professional development. The ES supports access to professional development.

No recommendation has been made as the current capacity and capability is optimal.

Topic 9: IM Roles and Responsibilities

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

Managing

Observations

Staff and contactor's IM responsibility is outlined in the Policy, though not in the Code of Conduct. Job descriptions sighted include reference to IM within their role's responsibilities. All job descriptions were reviewed and amended when the values statement was added and when an organisational review happens. This means that all have been reviewed in the last three years. As stated above, all staff undertake mandatory IM induction training, where the importance of IM is communicated, though no refresher training is done unless specifically requested. Senior staff understand their obligations, however are not confident if they are meeting good IM practice.

Recommendation

1. Provide refresher training for staff to increase confidence and technical knowledge on IM and raise awareness on the Ombudsman's IM resources.

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

Staff have a general understanding of their responsibility to create full and accurate information to support their business function. This is due to the induction training, nature of investigator's roles, ISSP, the Policy and services IKM provides. Feedback consistently stated most staff found information usable, reliable, and trustworthy. IKM does not actively monitor all repositories, however they conduct ad hoc checks and respond to any service requests.

Staff are also supported in fulfilling their responsibilities through the critical repositories used. Waka, which is used for corporate documents, is an enterprise content management system (ECMS) which meets the full Archives NZ metadata requirements. Also, a case management system (CMS) is used for capturing all complaints and investigations. The CMS is not classified as an ECMS. During the transition from paper case files to digital case files, the Ombudsman sought guidance from Archives NZ who confirmed that the system is fit-for-purpose.

The Ombudsman is currently implementing a new system to replace the CMS.

Shared drives are only used in read only function for historical records, as all required data has already been migrated to Waka or has been captured in legacy paper files. Staff do not have the ability to save any information within the shared drives.

There has been a recent initiative to create all information digitally, including case files, as outlined in the Paperless Office report. The majority of information is now digital, though some physical information is still sent in from complainants, but this is scanned and saved to the CMS on receipt.

Recommendation

1. Develop a regular review cycle of repositories to address any usability and reliability issues.

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.

Beginning

Observations

The IKM has started work on an Information Asset Register (IAR) to capture all information assets, including information classified as high-value / high-risk. The creation of an IAR is included in the IKM work programme and a pilot project is currently underway. Currently indexes of some physical files, their location, and some high-level lists of digital information indicate some identification of high-value / high-risk information.

Recommendation

1. Progress the pilot IAR to the whole organisation and develop a process for keeping it current.

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.

Managing

Observations

The IKM team is regularly involved in any new technology solutions and upgrades, due to close ties with the ICT team. This is shown through attendance of both IKM and ICT at the IMPSG, and the ISSP, which includes both teams' work programmes. All systems changes are approved through a Change Approval Board.

IKM is currently working closely with the project team on the new CMS. Their involvement is focused on ensuring metadata requirements are met and all IM requirements are addressed as the project progresses.

In 2017 there was a significant migration of data to a managed data centre, during the move to Waka. Throughout this migration IKM was heavily involved to ensure permissions were correct and data was moved effectively. The migration was considered a success.

Within the current CMS and Waka, there is a digital records management function on retention and disposal of information which has not been utilised. This function allows for information to be automatically kept per its retention requirements and flagged for deletion.

Recommendations

1. Use the current Disposal Authority to ensure the retention function in key repositories is utilised to meet the IM requirements.

2. Confirm the system replacing CMS meets metadata requirements and sufficient training is provided to staff to ensure information remains reliable and trustworthy.

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.

Managing

Observations

The reliability and trustworthiness of information is largely consistent across business areas. Certain roles, such as investigators, have thorough IM processes which supports the reliability of information. Staff interviewed noted they have a mostly consistent experience trying to find specific information and with version control.

A key improvement staff reported, which would increase the integrity of information, is a focus on improving naming conventions. This should include IKM developing guidance for each business unit and providing refresher training on good practice.

Recommendation

1. IKM to consult with business units to improve naming conventions.

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

IKM is regularly involved in any business and system changes. The Policy is currently being updated to formalise this requirement.

General accessibility to physical information is ensured through long-term ongoing storage, which is retained off-site with a commercial storage provider. The Ombudsman retains a summary of contents and an index of all physical information transferred to off-site storage to ensure information is still accessible to request back.

Security processes and continuous updates of systems ensure digital information remains accessible over time. Any new software must undertake an Information Risk Assessment, and a Security Risk Assessment. The CMS replacement project has considered technology updates and long-term adaptability in its development.

A clear formalised process to manage and maintain digital information during business and system changes is not in place. The Paperless Office report addresses how the Ombudsman should consider managing and maintaining physical information.

Recommendations

1. Include guidance on maintaining and managing information.

2. Update the Policy to formalise IKM involvement in business or system changes.

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.

Progressing

Observations

The Ombudsman has a business continuity plan, the Business Impact Analysis (BIA). The BIA identifies key business units, some critical information for business function, recovery time objectives and vital resources. It was last updated in 2021.

Digital backups are sent to separate storage and offline storage. Backups occur hourly, daily, weekly, monthly, and yearly. The previous week backups are stored offsite and easily retrievable. Currently backups are kept indefinitely. There is regular quarterly testing of digital system backups to ensure information can be restored.

Recommendations

1. Ensure sure all critical information is identified and addressed in the BIA.

2. Assess the risks of keeping backups indefinitely and decide on a retention period.

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.

Managing

Observations

The Ombudsman currently has 37,000 physical files stored with a third-party storage provider, which will be transferred to Archives NZ when the repository accepts physical transfers.

Physical information kept onsite is stored in lockable cabinets in the office, or in a secure storage room on the ground floor. It is stored in an office environment, which includes fire safety, flood mitigation and access control. Monthly access card reports to the ground floor files are reported to Senior Management. The information is labelled and indexed on the CMS. Any physical and information security breaches are reported to the Security Governance Committee (SGC) and mitigation actions tracked. A learning opportunity briefing may be announced on Awa, or at the Chief Ombudsman's staff briefing if appropriate.

A large portion of digital information storage is managed through third-party providers. The main IT provider is LANWorx and information security and protection requirements are built into the service contracts. The Ombudsman has a data centre in Wellington and Auckland, where data is duplicated. No information is stored offshore.

Recommendation

1. Undertake regular security testing and reporting of digital storage protection.

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.

Managing

Observations

The Ombudsman applies access controls for both physical and digital information. Access controls are in place across all digital systems, including restricting access to folders within Waka and CMS. Requesting access permission is a rigorous process which is assessed through role requirements, which Senior Management approve and IKM implement. SMT receives regular reporting on privacy and security incidents where access has been breached, including what action has been taken to mitigate the risk and implement learnings for future prevention.

Increased access control at the Ombudsman improves the security of information, though an over-restriction of information can be a barrier to staff requiring certain information, which may be relevant to their role.

All staff reported that the current taxonomy set within their business units facilitates consistent findability of information. However, several were not aware of metadata or advanced searching techniques.

Physical information is restricted through swipe card access and lockable cabinets. Swipe card access reports are sent to Senior Management on a monthly basis.

Recommendations

1. Provide advanced training to staff which includes metadata requirements and advanced search techniques.
2. Regularly review access restrictions to ensure they are protecting security and are practical for the business.

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 NZ (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 Ombudsman has a current approved Disposal Authority (DA), last updated in 2019. The DA covers information relating to all business areas and applies to all formats. It is reviewed annually to ensure it is still up to date with any business changes.

Disposal is not actively championed at a senior level, and several staff were not aware of the details of the DA, or confident in their understanding.

Recommendation

1. Increase training for staff on what is covered by the DA and how to meet IM 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.

Progressing

Observations

Implementation of the digital records management function within Waka is being tested. This function will automatically retain information for its approved retention period and notify when this has ended. The General Disposal Authorities (GDAs) and DA retention period has been loaded into Waka. This is part of a wider project plan to improve management of digital information.

Physical disposal is implementation under the GDAs on an annual basis, with signed approval. No disposal has been implemented under the new DA. Actioning of digital disposal is part of the 2021-2022 work programme, and a project plan for implemented will be completed by the end of this financial year.

Recommendation

1. Annually review both digital and physical information for disposal and ensure all disposal is secure, complete, and irreversible.

Topic 22: Transfer to Archives New Zealand

Information of archival value, both physical or digital, should be regularly transferred to Archives NZ or a deferral of transfer should be put in place.

Progressing

Observations

The Ombudsman has a significant amount of information over 25 years old, which is of archival value. Between 1992 to 2011, the Ombudsman sent physical files to Archives NZ, but none since. Physical case files are reviewed annually and sent to third party storage while awaiting transfer to Archives NZ. As case files have been kept in digital format only for the last two years but none have met their minimum retention period for transfer yet. There is a small amount of digital

corporate information that may be transferred which have not. However, staff recognised this would be a beneficial action.

Recommendation

1. In conjunction with Archives NZ, develop a digital information transfer plan.

6. Summary of Feedback

This section sets out the Ombudsman's feedback pursuant to this PRA audit.

The Chief Ombudsman welcomes this audit under the Public Records Act 2005. The recommendations align with the work we are already doing to improve our maturity and we will be incorporating the recommendations into this year and next year's ISSP and IKM work plan to grow our maturity in line with Archives New Zealand's standards and frameworks.

Deloitte.

Te Rua Mahara o te Kāwanatanga
ARCHIVES NEW ZEALAND

13 June 2022

Archives New Zealand, 10 Mulgrave Street, Wellington
Phone +64 499 5595
Websites www.archives.govt.nz
www.dia.govt.nz

Peter Boshier
Chief Ombudsman
Office of the Ombudsman
Karen.carter@ombudsman.parliament.nz

Tēnā koe Peter

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the Office of the Ombudsman (the Ombudsman) 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.

This letter replaces our letter of 3 June 2022. The recommendations in the Appendix are updated to reflect the change in the audit report after further discussion between the Office of the Ombudsman and Deloitte. The correction in the audit report to Topic 10: *Creation and Capture of Information* removed one of the recommendations that had been included in this letter. That recommendation has now been removed.

Introduction

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.

The audit of the Ombudsman gives a high degree of confidence that you and your organisation are committed to delivering high-quality, trusted information to decision-makers, other government organisations and stakeholders. We trust that the audit process will reinforce the ongoing benefits resulting from this commitment. The audit report and this letter recommend changes to support improvement of your organisation's IM practices.

We are confident that you and your organisation are committed to delivering high-quality, trusted information to decision-makers, other public 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.

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 report shows IM in the organisation is well supported with most maturity level assessments in the Managing level and above. This is an example of what committed organisations can achieve in management of their information.

Your Information Services Strategic Plan (ISSP) part of your organisational strategic planning framework, provides direction for your IM programme that is supported by the Senior Management Team and the Board. This ISSP is well monitored, and we commend you on this strategic work. The strategy is supported by IM processes and staff with appropriate expertise.

The assessment of Topic 3: *Governance arrangements and Executive Sponsor* at 'Maturing' is an example of very effective application of the Executive Sponsor role in leading IM. The report suggests benefit from wider sharing of this good practice, which we fully endorse. We will be in touch to discuss how this could be progressed with your office and other organisations with high IM maturity.

Prioritised recommendations

The audit report lists 23 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 five 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 for the release 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 for a discussion about sharing the Ombudsman's successful approaches and 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, and we will contact your Executive Sponsor shortly in relation to this.

Nāku noa, nā

Honiana Love
Acting Chief Archivist Kaipupuri Matua
Archives New Zealand Te Rua Mahara o te Kāwanatanga

Cc Michelle King, Assistant Ombudsman Corporate Services
michelle.king@ombudsman.parliament.nz (Executive Sponsor)

APPENDIX

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
Governance	6: Te Tiriti o Waitangi	*Work with Rōpu Māori Hononga Hapori to incorporate Te Tiriti o Waitangi and align the Ombudsman's te ao Māori transformation work programme into the ISSP and IKM work programmes, specifically to identify information of importance of Māori*	Identification of information of importance to Māori could also be incorporated into the work on Topic 11: High-value/High-risk.
Creation	11: High-Value/High-Risk Information	*Progress the pilot IAR to the whole organisation and develop a process for keeping it current.*	And IAR can help understand current and future management needs of the Ombudsman's information in association with the organisation's disposal authority.
Management	12: IM Requirements built into Technology Solutions	*Use the current Disposal Authority to ensure the retention function in key repositories is utilised to meet the IM requirements.*	Control of digital information is important to ensure the system works efficiently and to prepare for digital transfer.
Management	14: Information Maintenance and Accessibility	*Update the Policy to formalise IKM involvement in business or system changes.*	This could be incorporated into the current Policy review.
Disposal	21: Implementation of Disposal Decisions	*Annually review both digital and physical information for disposal and ensure all disposal is secure, complete, and irreversible.*	Implementation of the project plan to action digital disposal is a useful next step.