Deloitte.

Te Tari Hara Tāware

Serious Fraud Office

Public Records Act 2005 Audit Report

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

Final Report

February 2024

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 Serious Fraud Office (the SFO). 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 SFO 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 SFO. 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

TE TARI HARA TĀWARE | SERIOUS FRAUD OFFICE

Te Tari Hara Tāware | the Serious Fraud Office (the SFO) is a public service department with a statutory mandate under the Serious Fraud Act 1990 to investigate and prosecute serious or complex fraud, including bribery and corruption. This scope of responsibility includes:

- Disrupting and deterring serious fraud and corruption through prevention, investigation and prosecution;
- The development of guidance and strategies to prevent and respond to financial crime and corruption; and
- A contribution to New Zealand's international obligations relating to financial crime and corruption.

The office focus on cases with a disproportionately high impact on the financial and economic wellbeing of New Zealanders.

The SFO currently employs 78 full-time employees (FTE) with offices in Auckland and Wellington.

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

- Case files for investigations and prosecutions
- Policy advice
- Prevention guidance and advice
- Cross agency assistance.

The Executive Sponsor (ES) is also the Deputy Chief Executive, Corporate and Legal, and is responsible for overseeing IM. They have been in this role since September 2023. Given the relatively small size of the SFO, there is no team dedicated to IM, but there are IM subject matter experts. An IM Governance group is in place which includes the ES, Corporate Services Manager, and Forensic Services Manager.

SUMMARY OF FINDINGS

We assessed the SFO'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	3
Progressing	4
Managing	9
Maturing	3
Optimising	1

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 December 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 SFO'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 SFO's maturity level for each topic area is highlighted under each of the respective areas. Ratings were based on the SFO'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 SFO. Te Rua Mahara is responsible for following up on the report's recommendations with the SFO.

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 SFO'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.

Assessed Maturity Level						
No.	Topic	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.

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.	Managing

OBSERVATIONS

The SFO has an Information and Records Management Strategy (the Strategy) which was adopted by the SFO's IM Governance Group (IMGG) in November 2023. The Strategy sets out what the SFO will do to improve information and records management systems with the goal of meeting the expectations of the Chief Archivist. These actions also come with the additional goal of supporting the SFO to disrupt and deter serious or complex fraud and corruption. Key objectives include conducting IM self-assessments, designing and implementing IM activities, encouraging best practice for IM, and regularly appraising and disposing of records.

The Strategy is supported by six guiding principles:

- The ES and the IMGG to actively champion IM initiatives
- Business owners and staff are to be supported to be responsible for the information they create, use, and maintain
- Staff must be encouraged and supported to appropriately document SFO functions and activities
- Business systems are to be designed with IM in mind
- Information the SFO holds must be easy to find, access and use
- The security of SFO information is a priority.

Senior management actively support the strategic direction of IM within the SFO. The IMGG own the Strategy and oversee its implementation. Due to the recent adoption of the Strategy, specific reporting on its progress has not yet been formally established.

RECOMMENDATION

Establish a roadmap identifying specific IM initiatives and activities in alignment with the Strategy.

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 SFO has an Information and Records Management Policy (the Policy), which senior management has approved. The Policy details roles and responsibilities for IM in terms of relevant systems, information accessibility, retention and disposal.

The Policy is informed by the Strategy and the principles set out in the Te Rua Mahara Standard. It also outlines the regulatory framework within which the SFO operates and the requirements that must be met under the PRA and other relevant legislation.

The Policy was approved in October 2023 and there is limited staff awareness, as it has not yet been fully socialised across SFO.

RECOMMENDATION

Ensure the Policy is appropriately communicated to all staff and contractors.

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.	Progressing

OBSERVATIONS

Members of the IMGG include the ES, who is the Chair, the Corporate Services Manager and the Forensic Services Manager. The IMGG is responsible for owning and promoting the Strategy and using IM reporting to inform strategic business decisions and first met in October 2023.

Most special projects at the SFO have an IM component and currently report to the SLT. Therefore, it has been proposed that the IMGG should be notified of project initiations and receive reporting on projects with an IM component. Reporting and communication lines are still being formally established and there has not yet been any reporting to the IMGG.

Staff interviewed noted that despite taking-up the role recently, the ES previously had informal IM oversight when they were the Chief Legal Advisor.

RECOMMENDATION

Establish regular reporting to the IMGG covering all IM initiatives and 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.	Maturing

OBSERVATIONS

Business owners' responsibilities for IM are outlined in the Policy. Their responsibilities include ensuring IM is implemented in the context of case management and corporate administration activities. Business owners are also responsible for ensuring employees are sufficiently trained and are made aware of the Policy.

More specific responsibilities for IM are also detailed for other roles. The Corporate Services Manager is responsible for providing guidance and training to employees on IM practices, policies, and systems. The Forensic Services and Human Resources teams are responsible for providing business support for implementing IM best practice as well as processing requests for SFO records. IM responsibilities are primarily communicated through the Policy and are not included in performance plans.

Business owners, some of which are members of the IMGG, are responsible for IT systems. It was reported that issues relating to IM which impact business systems are directed to the appropriate business owner who then escalate the issue to the ES, where needed. Business owners also play a part in reviewing folder structures, access permissions, and evidence management processes. IM is a significant consideration in business process changes and corporate and legal expertise are consulted through any changes. Most business process changes involve members of the IMGG who are responsible for ensuring IM requirements are addressed.

RECOMMENDATION

Ensure responsibility for management and quality of information is included in performance plans.

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.	Managing

OBSERVATIONS

The SFO has a range of contracts with third-party vendors. These contracts outline relevant legislation and include requirements and responsibilities for IM, usability and accessibility. These specifically include obligations relating to security and privacy breaches. IM responsibilities within contracts are identified and monitored.

Third parties are required to keep and maintain records in accordance with all applicable laws and ensure they are accurate, usable, and easily accessible.

Risks of non-compliance by any party in contracts are not formally identified or monitored.

RECOMMENDATION

Identify and address the risks of non-compliance with IM responsibilities 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 SFO has not identified information of importance to Māori. IM implications within Te Tiriti o Waitangi settlement agreements and other agreements with Māori are also not identified.

RECOMMENDATION

Develop processes to locate and identify information of importance to Māori.

SELF-MONITORING

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

Topic 7: Self-Monitoring

Organisations should monitor all aspects of their information management.	Progressing

OBSERVATIONS

The SFO conducts a range of self-monitoring activities. Reports against legal obligations are created using a third-party legal monitoring tool and are addressed to the Chief Executive. This results in roadmaps for improvement being created and actions being allocated to staff. There are also annual self-assessments against Protective Security Requirements (PSR). The Strategy states that the SFO plans to annually self-assess against the IM maturity assessment.

There is currently no framework in place for monitoring against internal policies and processes.

RECOMMENDATION

Establish a self-monitoring programme for IM and report results to the IMGG.

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.	Managing

OBSERVATIONS

Due to its relatively small size, the SFO does not have a dedicated IM team. Despite this, staff interviewed reported that there is sufficient IM capacity and capability in the organisation to meet business needs. There is budget for professional development for all staff, much of which is mandatory for Legal staff, as they have responsibility for IM. This includes developing in areas relating to IM such as privacy and security.

The ES stated that there is sufficient capacity to be involved in projects or initiatives where IM input is needed.

RECOMMENDATION

Ensure IM capacity and capability needs are regularly assessed and addressed to meet future business needs.

Topic 9: IM Roles and Responsibilities

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

OBSERVATIONS

IM training is included in induction for new staff and contractors. On-going training involves refreshers on the use of case and evidence management systems. There is also regular training provided on IM related matters such as privacy, security, and confidentiality.

IM roles and responsibilities are largely well understood by staff, with roles and responsibilities only communicated through the Policy and related guidelines but not in job descriptions.

RECOMMENDATION

Regularly review and update job descriptions and performance plans to ensure they include IM roles and responsibilities.

CREATION

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

Topic 10: Creation and Capture of Information

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

OBSERVATIONS

The primary Electronic Document Management System (EDMS) used at the SFO is a SharePoint based system. The EDMS is used for the storage of records relating to investigations and prosecutions as well as corporate information, including emails. This system is linked to a case management system and an evidence management system.

These systems require sufficient metadata to be entered before information is stored. Where possible staff will add metadata to information being stored in the EDMS as a matter of good practice. Because of this, staff reported no significant barriers to accurately capturing information and expressed confidence in their ability to do so. There is not yet any reporting to the IMGG of any issues relating to the usability and reliability of information.

Staff have a strong awareness of their legal obligations as public servants to create and capture full and accurate information. This is largely born out of the necessity to do so for the success of investigations and prosecutions. Training on relevant systems is provided and staff are required to use approved IM systems in carrying out their responsibilities. This is monitored by IT staff who are alerted if any staff attempt to download information using unapproved systems.

RECOMMENDATION

Establish reporting requirements to the IMGG on organisation-wide usability, reliability, and trust issues for resolution.

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

There is some identification of high-value/high-risk information assets in an information asset register (IAR). This includes details on the custodianship, context, value, and security and privacy considerations for information assets.

RECOMMENDATION

Complete the identification of all high-value/high-risk information assets in the 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 when decommissioning technology systems. This is largely through communicating requirements and IM needs with system vendors as well as through completing the GCDO cloud assessment for new cloud-based systems. Disposal processes and metadata are built into case and evidence management systems as well as the EDMS. This facilitates the retention of information of long-term value.

While exit strategies are not explicitly included when planning new systems or upgrades, agreements are regularly reviewed to ensure they meet current needs. This means that when system and application contracts expire, there is the possibility to either renew or exit subscriptions with IT vendors.

A recent task involving the decommissioning of a system included IT staff and IM expertise. The task involved migrating data to a new server and running checks on information between the two systems to verify the integrity of the information. Risks relating to this system and other systems that do not meet IM requirements are identified and there are plans to address these.

Te Rua Mahara minimum metadata requirements are met in case and evidence management systems as well as in the EDMS.

RECOMMENDATION

Ensure that risks relating to business systems that do not meet IM requirements are mitigated.

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.	Optimising

OBSERVATIONS

A high value is placed on ensuring that information that is created and managed is trustworthy, findable, and retrievable. This is due to the critical nature of much of the information that SFO holds. The success of investigations and prosecutions depends heavily on the quality and integrity of the information that is presented to courts by the SFO. Therefore, staff place a significant level of importance capturing information so that it is accurate and easily findable in the future. Throughout the organisation, information is filed and given a tracking number making it easy to find throughout its lifecycle. This is overseen by the evidence management team and any issues are reported to the IT manager.

Staff advised that they have reliable and consistent experiences when using information from across the organisation. There were no barriers to finding information reported, nor could any instances of not being able to find information be recalled. This is also due to how the EDMS and interrelated systems are set up. All evidence is given a tracking number which is linked to the relevant case. Information also has significant metadata which must be attached to aid in the retrieval of information.

The taxonomy in the EDMS is fit-for-purpose and is reviewed and updated when needed. Corporate records held here include descriptive metadata and document versioning. There is also a system in place for storing email communications.

RECOMMENDATION

There is no recommendation for this topic due to the maturity rating of optimising.

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.	Managing

OBSERVATIONS

All of the SFO's significant information in physical format is maintained by their third-party storage provider.

There is work being planned to ensure digital information is maintained and can be accessed over the long-term. This will involve moving information from obsolete systems to cloud-based systems. Until this project is initiated, there is a focus on retaining digital information.

RECOMMENDATION

Ensure preservation and continuity needs for digital information are addressed.

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

All critical information is stored in digital format.

The SFO's Business Continuity Plan (BCP) was last updated in September 2023, with roles and responsibilities defined for a business disruption event. Individuals on the IMGG are responsible for securing access to IM systems and working with relevant team members to restore information. The BCP includes procedures and plans for restoring digital information. There are regular reviews and updates of the BCP, however, critical information for business continuity is not formally identified here.

Backups of digital information are conducted and tested regularly. The SFO also have access to incident response expertise for urgent events for restoring information following a business disruption event.

Staff have a strong understanding of their responsibilities as defined in the BCP. Those on the SLT and the IMGG, as well as IT staff were involved in the establishment of the BCP.

RECOMMENDATION

Ensure the BCP formally identifies critical information required for business continuity.

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

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

The majority of digital information is held overseas and reported on in the PSR assessment. Penetration testing is conducted annually and the GCDO cloud risk assessment is also completed for new cloud-based solutions. There are a range of mechanisms employed to protect information from unauthorised access or loss. These include access controls and retention policies built into IM systems.

While there have been no significant digital protection and security breaches, there are processes in place for responding to these. Any new access permissions, instances of deletion, or use of personal systems automatically notify IT staff who escalate any issues to the ES where needed. There are also weekly meetings between IT and the Chief Security Officer where any risks and issues are discussed. These may also be discussed at information security committee meetings.

RECOMMENDATION

Test protection and security processes regularly.

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

There are memorandums of understanding in place for information sharing with other public sector agencies. These outline criteria and processes for sharing information using secure platforms. A non-disclosure agreement is in place where information is shared with third parties.

Internally, staff reported no barriers to finding the information they need to do their work. This is in-part due to significant metadata and folder structures being intuitive and easy to use. Descriptive metadata is often added to information in the case management system which is linked to the tracking numbers attached to evidence. It was also noted that the small size of the organisation means staff always have access to IM assistance when they need help searching for information.

Staff reported that they have appropriate access permissions to carry out their responsibilities. While controls and processes are in place, they are not formally documented for all systems. Certain case information is generally open access across the organisation and in some circumstances staff are only granted access to information relevant to cases they are assigned. Case leaders are able to provide access to sensitive information to staff with sign-off from a manager. Certain access permissions are overseen by IT staff who are notified of any new access requests. There are regular audits of access permissions which are included in PSR reporting.

RECOMMENDATION

Document controls and processes for access controls across all systems.

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.	Progressing

OBSERVATIONS

The SFO does not currently have an approved Disposal Authority (DA). There is a draft Appraisal Report and Disposal Schedule currently with Te Rua Mahara for review.

RECOMMENDATION

Prioritise the completion of the disposal authority when received from Te Rua Mahara.

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.	Beginning

OBSERVATIONS

Work is planned to appraise records to be disposed of or retained once the DA is approved. There is no disposal under General Disposal Authorities. This is due to the SFO waiting for the organisation-specific DA to be approved before organising disposals under one program of work.

RECOMMENDATION

Develop a disposal plan to implement across all formats and repositories where possible.

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

No transfers have occurred since 2014. There are plans to assess historic records and formalise transfers once there is an approved DA. Information of archival value that is over 25 years old has not been identified.

RECOMMENDATION

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

6. Summary of Feedback

Efficient and effective information and records management is essential to enable the SFO to meet its strategic objectives and to prevent, investigate and prosecute serious fraud.

Our move to a purely digital environment brings new challenges, which we have addressed with the establishment of an Information Governance Group and a refresh of our Information Management Policy. Archiving activities for paper holdings will re-commence on receipt of an updated Disposal Authority.

We continue to strive to demonstrate a best practice approach to information management, including in the design of our systems and processes, and will assess our capability once a year against the Archives NZ Information Maturity Assessment.

Deloitte.

Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND

18 March 2024

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

Karen Chang
Director and Chief Executive
The Serious Fraud Office
Te Tari Hara Tāware
karen.chang@sfo.govt.nz

E te rangatira e Karen, tēnā koe

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of Te Tari Hara Tāware the Serious Fraud Office (SFO) 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.

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 SFO is assessed with IM Maturity across the maturity spectrum with nine topics at 'Managing' level, seven topics below that and four above.

The organisation highly values its operational information in supporting it to perform its key tasks well. An IM framework developed in 2023 includes an Information and Records Management Strategy and Policy and established the IM Governance Group. We commend the intention to undertake annual reviews using the IM Maturity Assessment.

When the organisation-specific disposal authority is approved, its application through disposal including transfer to our digital and Auckland (physical) repositories will require resourcing. This should be included in the roadmap for implementation of the Information and Records Management Strategy.

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 seven 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 Kylie Cooper, Deputy Chief Executive Corporate and Legal (Executive Sponsor), kylie.cooper@sfo.govt.nz

APPENDIX

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Governance	I: IM Strategy	*Establish a roadmap identifying specific IM initiatives and activities in alignment with the Strategy.*	The establishment and implementation of the roadmap will provide the basis for reporting on the Strategy and upholding the six guiding principles.
Governance	2: IM Policy	*Ensure the Policy is appropriately communicated to all staff and contractors.*	This will ensure that the expectations and requirements of the Policy are understood across the organisation.
Governance	3: Governance Arrangements and Executive Sponsor	*Establish regular reporting to the IMGG covering all IM initiatives and activities.*	This will ensure that awareness of IM activity and issues is well understood by those on the group.
Governance	6: Te Tiriti o Waitangi	*Develop processes to locate and identify information of importance to Māori.*	This area should at least be considered to determine what information of importance to Māori is held and what work needs to proceed from there.
Self-Monitoring	7: Self-Monitoring	*Establish a self-monitoring programme for IM and report results to the IMGG.*	This is an important next step to ensure that trends and issues are identified, monitored and addressed as needed.
Capability	8: Capacity and Capability	*Ensure IM capacity and capability needs are regularly assessed and addressed to meet future business needs.*	When the work plan for the Strategy is developed the resourcing will need to be considered.
Creation	11: High-Value/High-Risk Information	*Complete the identification of all high-value/high-risk information assets in the IAR.*	This will enable the organisation to understand its information and prioritise its IM work. This can be done in conjunction with the organisation-specific disposal authority.

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Disposal	21: Implementation of Disposal Decisions	*Develop a disposal plan to implement across all formats and repositories where possible.*	The plan will need to be approved and implemented to ensure that the organisation realises the benefit of having the organisation-specific disposal authority.