



# Guardians of New Zealand Superannuation Public Records Act 2005 Audit Report

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

May 2024



# Table of Contents

1. Disclaimers	2
2. Executive Summary	3
3. Introduction	4
4. Information Management Maturity Summary	5
5. Audit Findings by Category and Topic	6
Governance	6
Self-monitoring	8
Capability	10
Creation	11
Management	13
Storage	14
Access	16
Disposal	16
6. Summary of Feedback	19

# 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 Guardians of New Zealand Superannuation (the Guardians). 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 Guardians 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 Information Management (IM) Maturity Assessment of Te Rua Mahara.

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 Guardians. 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

### GUARDIANS OF NEW ZEALAND SUPERANNUATION

Guardians of New Zealand Superannuation (the Guardians) is a Crown entity established under the New Zealand Superannuation and Retirement Income Act 2001 (the Act). The Guardians report to the Minister of Finance each quarter and is governed by its Board.

The Act provides the Guardians with a mandate to invest the NZ Super Fund on a prudent and commercial basis. This is to be achieved in a manner consistent with best practice, maximising returns and avoiding prejudice to New Zealand's reputation. The Guardians two primary functions are to:

1. Invest the money the Government has contributed to a growth-orientated and diversified global portfolio of investments via the New Zealand Superannuation Fund.
2. Contribute to a sustainable and productive economy through increasing the amount of capital available to New Zealand entities through the Elevate NZ Venture Fund.

The Guardians holds high-value/high-risk information including:

- On its Superannuation schemes
- Legislation submissions and legal opinions.

The Executive Sponsor (ES) is the General Manager Risk, who has been responsible for the information management (IM) at the Guardians since 2021. There are 213 full-time equivalents (FTE) all located at its head office in Auckland.

### SUMMARY OF FINDINGS

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

#### Maturity Level and Number of Findings

<b>Beginning</b>	-
<b>Progressing</b>	11
<b>Managing</b>	6
<b>Maturing</b>	2
<b>Optimising</b>	-
<b>Not Applicable</b>	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.
- 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 March 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 Guardians' IM practices against the IM Maturity Assessment. The IM Maturity Assessment aligns with the PRA and the mandatory Information and records management standard (the Standard) issued by Te Rua Mahara. Topics 17 and 19 of the IM Maturity Assessment are only applicable to local authorities and have therefore been excluded for the purposes of this audit.

The IM Maturity Assessment classifies the maturity of IM practices from "Beginning" (least mature) to "Optimising" (highest maturity level). The maturity level of the Guardians for each topic area is highlighted under each of the respective areas. Ratings were based on responses from the Guardians staff 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. Deloitte completed the onsite audit and audit report, which Te Rua Mahara reviewed before being released to the Guardians. Te Rua Mahara is responsible for following up on the report's recommendations with the Guardians.

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.

Feedback from the Guardians to this report is set out in Section 6.

## 4. Information Management Maturity Summary

This section lists the IM 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	Not Applicable				

**Note:** Topics 17 and 19 of the 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 Guardians has a current IM Strategy (the Strategy), which outlines its strategic goals and direction for IM and includes an implementation plan. The Strategy includes goals for uplifting IM maturity and was an input into the programme to modernise the Guardians’ workplace. This also includes applying aspects of Te Rua Mahara Maturity Self-Assessment to its IM approach. The Strategy was approved in October 2023 and is due for review in 2025.

The Knowledge Manager (KM) tracks IM initiatives progress in the Strategy by reviewing the relevant completed actions.

Senior management are aware of, and actively support, the IM strategic direction.

#### RECOMMENDATION

Ensure that the Strategy is regularly assessed to ensure the objectives are relevant, initiatives are resourced, and outcomes are measurable, in line with the broader Guardians strategic direction.

### 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.	Progressing
--------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------

#### OBSERVATIONS

The Guardians has an IM Policy (the Policy) and related Information and Records Management (IRM) Standards and Procedures Manual (the Manual). Both are awaiting sign off from Senior Management. The Policy includes links to other policies such as Security and Privacy.

Roles and responsibilities for IM are included in the Manual, which is intended to be read alongside the Policy. The Manual also includes documented IM processes.

#### RECOMMENDATION

Approve the Policy and Manual and communicate 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.

Managing

#### OBSERVATIONS

The Guardians' ES is the General Manager Risk and actively champions IM. The ES was previously supported by external IM consultants and a prior IM staff member and, for the last five months, support has been from the KM. The ES has been in their role for three years and is aware of their oversight and monitoring role and is a member of the IM governance group.

The Guardians recently established an IM governance group, the Knowledge Governance Group (KGG), which includes senior members of the Guardians' leadership team and met for the first time in February 2024. The purpose of the KGG is to provide a forum for ongoing management, continuous improvement and maturity of the Guardians' IM framework. The KGG Terms of Reference includes reference to the mandatory Information and records management standard and the Guardians own internal IM principles.

The ES receives some formalised reporting on IM initiatives and programmes, such as adoption reports for SharePoint sites and would receive notifications for any IM incidents through Learning Opportunity Reports (LORs). These LORs would be used to provide learning opportunities for all after an incident.

#### RECOMMENDATION

Ensure the reporting to the ES identifies issues that need addressing so that they can be acted on.

### 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

The Guardians is well advanced in transitioning their main Electronic Document Management System (EDMS) from eDocs to SharePoint. This transition will enable automatic versioning and metadata for documents created in SharePoint and additional reporting capability. Other core systems include ServiceNow and Oracle HCM used for IT and HR business purposes respectively and are considered controlled systems called Approved Information Management Systems (AIMS). These systems are considered appropriate for document storage, as they comply with the Guardians' internal IM principles which includes minimum metadata requirements. The Guardians staff only use AIMS for using and maintaining their information, ensuring that IM is integrated into their business processes and activities.

IM roles and responsibilities are included in job descriptions at a high level, except for certain roles, such as Legal, which are in more detail. Responsibility for IM within business units will be formalised for business owners following the approval of the Policy and Manual. However, staff have expressed an understanding of these responsibilities.

Both eDocs and SharePoint meet minimum metadata standards, and SharePoint automatically applies metadata to documents created.

The KM is currently focused on improving IM maturity through an IM uplift to support business processes and activities. IM expertise is beginning to be included in business process change and development, as the



ES invites the KM to meetings where their input would be useful, and staff are starting to come to the KM for assistance with this.

#### RECOMMENDATION

Encourage business owners to actively fulfil their responsibilities for IM 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 Guardians has contracts with third parties for outsourced business functions and services. Sighted contracts include general IM details and requirements relating to confidentiality, data integrity and security. IM roles and responsibilities were included at a high level in some sampled contracts but not all.

The Guardians can monitor contracts including IM requirements, but this is not a regular practice.

#### RECOMMENDATION

Monitor IM requirements in contracts for outsourced functions and collaborative arrangements where appropriate.

### 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.	Progressing
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------

#### OBSERVATIONS

The Guardians is aware that some information they hold is of importance to Māori. They have also completed a process to identify and document where relationships with iwi exist. Furthermore, the ES and KM intend to update metadata fields in SharePoint to improve findability of information that is of importance to Māori.

#### RECOMMENDATION

Continue identifying information of importance to Māori and implement changes to IM practices to improve access, discoverability and care.

## 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

In February 2024 the Guardians completed a review of legislative compliance using an external third party. Also, in September 2023 it reviewed its systems level of compliance against their internal AIMS categorisation. In the future the Guardians intend to regularly monitor IM processes, systems and activities as part of their Strategy.

The KM produces adoption reports for SharePoint and is actively exploring other reporting options which may be of value to the ES and KGG. Previously, the Records Manager provided regular reporting to the ES and business owners on the number of documents saved by teams, however this ended when the Records Manager left.

The KGG has recently given feedback to the KM on what forms of reporting they would like to receive going forward. This includes types of records saved, number of records, and retention and disposal information. The KM is currently developing other reporting in SharePoint which will be provided to the ES and ultimately the KGG.

The ES and other members of the KGG would be notified if there were any incidents or breaches of security through LORs as part of their business as usual (BAU) roles. When a corrective action is required, there is a structured approach to implementing these through the LORs.

#### RECOMMENDATION

Agree and regularly implement IM monitoring and reporting to KGG.

## 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

The KM is currently the only internal IM staff member and is supported in their role by the ES. The Guardians has previously used external IM consultants, including in the initial stages of the eDocs migration. They do contract external IM consultants if additional support is needed. The KM started five months ago to support IM uplift across the organisation. At the time of the KM's recruitment, the Guardians had assessed their IM capability and capacity and noted a need for an IM staff member after the prior IM staff member left. IM capability and capacity will be reviewed following the transition from eDocs to SharePoint to determine if further IM capacity or capability is required.

All employees have access to a professional development budget and the KM has had the opportunity to attend IM-specific events.

#### RECOMMENDATION

Review IM capacity and capability following the transition to SharePoint to ensure that this is aligned to current and future business needs.

### Topic 9: IM Roles and Responsibilities

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

Progressing

#### OBSERVATIONS

Roles and responsibilities for IM are included in job descriptions, the draft Policy and draft Manual.

The KM undertakes induction training on IM. Training on systems such as SharePoint was provided when the system went live. Prior to the KM starting, training on system usage was provided by the Technology team.

There are intranet articles on IM, which are published as a part of the modernising workplace programme. However, there is no formal ongoing programme of IM training.

#### RECOMMENDATION

Identify ongoing training needs for IM and develop a plan to deliver targeted training in response to business needs and issues.

## 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 Guardians is currently in the process of transitioning to SharePoint as their main EDMS, with most teams now using it. While information is largely held on eDocs or SharePoint, other documents such as contracts and HR information are maintained on AIMS-classified systems. Staff are aware of their responsibilities for creating, capturing and managing information.

Staff reported frequent collaboration between business units. Experiences with creating and capturing information was consistent between business units, and one team maintains a central directory to ensure accessibility of final contractual documents. As part of the SharePoint transition, the taxonomy used by the business has been updated to a functional taxonomy which is applied across the organisation. Staff noted that they were still in the process of familiarising themselves with this new taxonomy as some documents appeared to be suitable for multiple folders. This may create a concern around information findability or reliability.

SharePoint and eDocs comply with minimum metadata requirements. External USB drives are disabled on laptops and there is a policy on how to manage data outside of the Guardians' IT environment. In the event of an issue relating to IM, LORs can be raised to address educational uplift or technical issues. LORs are raised by exception.

#### RECOMMENDATION

Monitor and address any usability, reliability and trust issues arising from transition to SharePoint.

### 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 Guardians has an inventory documenting information held in systems such as SharePoint and eDocs, at a high level, and are in the process of creating an Information Asset Register (IAR). This has been discussed by the KGG and is included in the Strategy.

There has been some identification of high-risk/high-value assets.

#### RECOMMENDATION

Work with business owners to identify high-risk/high-value information assets and complete 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.

Progressing

#### OBSERVATIONS

The Guardians involved IM consultants in the introduction of SharePoint and have installed a third-party IM/record-keeping module on their SharePoint. There is a migration plan for eDocs which includes reference to metadata requirements and plans for data reconciliation. Both SharePoint, eDocs and AIMS meet minimum metadata requirements. Standardised minimum metadata requirements will be formalised in the Policy and Manual and are required for the controlled systems.

System documentation does not exist for all business systems but are created and maintained for newer systems including Standard Operating Procedures (SOPs).

#### RECOMMENDATION

Create and maintain business system documentation for all 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.

Managing

#### OBSERVATIONS

Staff interviewed were confident in the integrity of information available within SharePoint and eDocs and noted no major barriers to finding information and records across teams. SharePoint has auto-versioning controls for documents created within it and there is enterprise search across Microsoft systems such as SharePoint and Outlook. Staff use controlled systems for their documents and did not report using personal drives for IM.

Due to the transition from eDocs to SharePoint, there is an opportunity to embed organisation-wide IM practices through training on the use of SharePoint and consistent use of the new taxonomy.

Staff are required to attest that they are complying with all policies, such as the security and privacy policy, at six-monthly intervals. This attestation will include the Policy when this has been finalised.

Following an LOR, system controls would be reviewed, if necessary.

## RECOMMENDATION

When SharePoint is fully operational, monitor user-experience to understand and address any issues with finding and retrieving information.

### 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

The Guardians hold the majority of its physical information off-site with a third-party storage provider. There is also a small amount of physical information held onsite with regular temperature and humidity monitoring. Onsite storage has a hazard register maintained by the building manager and access is limited to authorised staff which can be monitored.

The Guardians do not currently have a Digital Continuity Strategy, or other digital continuity plan, although strategies are in place for managing and maintaining information during the system change from eDocs to SharePoint, including discussions of metadata continuity.

## RECOMMENDATION

Identify digital continuity needs and develop a plan to address these.

### 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

The Guardians has an organisation wide Crisis Management Plan (CMP) which includes business recovery and was last updated in January 2024. Both the ES and KM reviewed and contributed to it. The CMP includes plans for restoring digital information and providing remote access for staff to required systems. Systems which hold critical information have been identified within the CMP, as have critical activities performed by each team. Salvaging and restoring physical information was discussed during a recent emergency exercise, but it was decided that this is not a priority. This was because any physical information stored onsite has been digitised. Other physical information is stored at a third-party storage provider.

There are daily back-ups stored across two geographic locations using servers which are able to replicate data. There was a partial test of restoration within the last 18 months, and a full test is being planned for within the next three months. Back-ups taken are stored on Australian servers.

## RECOMMENDATION

Ensure any issues identified during testing of business continuity and recovery plans are remediated.

## 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 Guardians hold a small amount of physical information onsite in an access-controlled room. The floor requires token access which is limited to Guardians employees and access to the storage room is restricted only to applicable staff. This room has fire protection and files are stored in appropriate shelving. Temperature and humidity readings are regularly taken and monitored.

Digital information is stored on controlled systems and is protected by access controls and a soft-delete function which enables recovery of accidentally deleted documents. In addition, a third-party is responsible for accessing and managing audit logs for all systems including for any unauthorised access or breaches.

As the KGG has recently been established they have yet to be informed of the information protection and security risks.

#### RECOMMENDATION

Ensure that information protection and security risks are regularly reported to the KGG, and remediation actions are identified.



## 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.	Maturing
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------

#### OBSERVATIONS

As part of the transition from eDocs to SharePoint, the Guardians has updated their taxonomy. This included a move from a business unit taxonomy to a functional one which is consistent across the organisation. This taxonomy is being actively monitored and adjusted during the transition from eDocs to SharePoint. Metadata is automatically applied within SharePoint, but staff can add additional tags if appropriate. Staff stated that they have been provided training on metadata and search techniques for the new SharePoint system.

Access controls for digital information are updated on a quarterly basis and the ES has oversight of access controls through their BAU role. Staff access can be restricted from files they do not need to access and access permissions are changed when a role changes or someone new comes onboard. As a result, no issues with access controls were raised in interviews.

IM processes are applied to some incoming and outgoing information shared with third parties. This includes sharing of confidential information over email and through restriction of the use of USBs and services such as Dropbox.

#### RECOMMENDATION

Develop a process for active maintenance of the taxonomy going forwards.

## 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 Te Rua Mahara (or have a deferral of transfer) and be determined as either “open access” or “restricted**

### 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 Guardians does not have a current organisation-specific Disposal Authority (DA). They have drafted one which has received initial feedback from Te Rua Mahara and is now awaiting their approval.

#### RECOMMENDATION

Finalise the organisation-specific DA and send to the Poumanaaki Chief Archivist for approval.

### 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

The Guardians has not completed any disposal of digital information and are developing a process for regular disposal through a third-party IM tool.

The Guardians has disposed of physical information through their third-party storage provider under its General Disposal Authorities (GDAs). Disposal of information requires three signatures for sign-off and deletion only occurs once this form has been completed. The final sign-off is with the KM for all disposal actions and this disposal will then be entered on the disposal register.

#### RECOMMENDATION

Develop and implement a disposal plan for digital and physical information once the organisation-specific disposal authority is approved.

**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.

Not Applicable
-------------------

**OBSERVATIONS**

The Guardians was established in 2001 and therefore have no information which is over 25 years old.

**RECOMMENDATION**

Not Applicable.

## 6. Summary of Feedback

The Guardians of New Zealand Superannuation would like to thank Te Rua Mahara o te Kāwanatanga Archives New Zealand and Deloitte for their work on this audit, the recommendations, and the direction this will give to our future work improving and maturing our IM practices.

Overall, we consider the audit to be a fair evaluation of our information maturity. The Guardians are committed to robust IM and we are pleased that the audit validates our own maturity self-assessment. Most of the recommendations align to work we already have underway or planned and reinforces that our focus is the correct one.

The audit has been timely with the implementation of our new technology environment and the establishment of the Knowledge Governance Group. It will provide a useful benchmark for measuring the uplift in our IM practices over time and we look forward to developing an action plan with Te Rua Mahara o te Kāwanatanga Archives New Zealand.



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organisation”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s approximately 415,000 people worldwide make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

Deloitte New Zealand brings together more than 1800 specialist professionals providing audit, tax, technology and systems, strategy and performance improvement, risk management, corporate finance, business recovery, forensic and accounting services. Our people are based in Auckland, Hamilton, Rotorua, Wellington, Christchurch, Queenstown and Dunedin, serving clients that range from New Zealand’s largest companies and public sector organisations to smaller businesses with ambition to grow. For more information about Deloitte in New Zealand, look to our website [www.deloitte.co.nz](http://www.deloitte.co.nz).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organisation”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2024. Deloitte Limited (as trustee for the Deloitte Trading Trust).

03 September 2024

Te Rua Mahara o te Kāwanatanga Archives New Zealand

10 Mulgrave Street

Wellington

Phone +64 499 5595

Websites [www.archives.govt.nz](http://www.archives.govt.nz)

[www.dia.govt.nz](http://www.dia.govt.nz)

Matthew Ludlow Whineray

Chief Executive

Guardians of New Zealand

Superannuation

[mwhineray@nzsuperfund.co.nz](mailto:mwhineray@nzsuperfund.co.nz)

E te rangatira e Matthew, tēnā koe

## Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the Guardians of New Zealand Superannuation (the Guardians) 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 Guardian's IM practice is assessed as mostly at Progressing maturity.

Currently the move to SharePoint is your key work in improving IM maturity. It is essential for a successful transition that the system is monitored, and trends and issues in its use are addressed as needed. An example of this is the use of the new functional taxonomy applied to SharePoint. Training is needed so that staff understand how to use it, its use is monitored and any issues arising are addressed through training.

## 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 Mark Fennell, General Manager Finance and Risk (Executive Sponsor),  
[MFennell@nzsuperfund.co.nz](mailto:MFennell@nzsuperfund.co.nz)

## APPENDIX

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
<b>Governance</b>	2: IM Policy and Processes	<i>Approve the Policy and Manual and communicate to all staff and contractors.</i>	This provides a basis for consistent understanding of IM practice across the organisation.
<b>Self-Monitoring</b>	7: Self-Monitoring	<i>Agree and regularly implement IM monitoring and reporting to KGG.</i>	This will support the ES in their role and ensure that the KGG has the relevant information needed to support IM throughout the organisation. This will also improve the maturity of Topic 3: <i>Governance Arrangements and Executive Sponsor</i> .
<b>Capability</b>	8: Capacity and Capability	<i>Review IM capacity and capability following the transition to SharePoint to ensure that this is aligned to current and future business needs.</i>	IM improvement hinges on having the right level of resourcing so this is a key activity. Resource needed to implement the Strategy and support the new SharePoint environment should be assessed and met where possible.
<b>Capability</b>	9: IM Roles and Responsibilities	<i>Identify ongoing training needs for IM and develop a plan to deliver targeted training in response to business needs and issues.</i>	This is especially important to support the transition to SharePoint and effective use of the new taxonomy.
<b>Creation</b>	11: High-Value/High-Risk Information	<i>Work with business owners to identify high-risk/high-risk information assets and complete the IAR.</i>	This will help in managing the organisation's most important information.
<b>Disposal</b>	20: Current Organisation-Specific Disposal Authorities	<i>Finalise and send the organisation-specific DA to the Poumanaaki Chief Archivist for approval.</i>	As this has had considerable work already it would be beneficial to complete asap.



Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
<b>Disposal</b>	21: Implementation of Disposal Decisions	<i>Develop and implement a disposal plan for digital and physical information once the organisation-specific disposal authority is approved.</i>	This will allow the organisation to realise the benefit from the work developing the DA and manage storage costs.