Public Records Audit Report for the Ministry of Defence

Prepared for Te Rua Mahara o te Kāwanatanga Archives New Zealand

March 2023

kpmg.com/nz

Disclaimers

Inherent Limitations

This report has been prepared in accordance with our Consultancy Services Order with Te Rua Mahara o te Kāwanatanga Archives New Zealand dated 26 November 2020. Unless stated otherwise in the CSO, this report is not to be shared with third parties. However, we are aware that you may wish to disclose to central agencies and/or relevant Ministers' offices elements of any report we provide to you under the terms of this engagement. In this event, we will not require central agencies or relevant Ministers' offices to sign any separate waivers.

The services provided under our CSO ('Services') have not been undertaken in accordance with any auditing, review or assurance standards. The term "Audit/Review" used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The information presented in this report is based on that made available to us in the course of our work, publicly available information, and information provided by Te Rua Mahara o te Kāwanatanga Archives New Zealand and the Ministry of Defence. We have indicated within this report the sources of the information provided. Unless otherwise stated in this report, we have relied upon the truth, accuracy and completeness of any information provided or made available to us in connection with the Services without independently verifying it.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, the Ministry of Defence management and personnel consulted as part of the process.

Third Party Reliance

This report is solely for the purpose set out in Section 2 and 3 of this report and for Te Rua Mahara o te Kāwanatanga Archives New Zealand and the Ministry of Defence's information and is not to be used for any other purpose or copied, distributed or quoted whether in whole or in part to any other party without KPMG's prior written consent. Other than our responsibility to Te Rua Mahara o te Kāwanatanga Archives New Zealand, neither KPMG nor any member or employee of KPMG assumes any responsibility, or liability of any kind, to any third party in connection with the provision of this report. Accordingly, any third party choosing to rely on this report does so at their own risk. Additionally, we reserve the right but not the obligation to update our report or to revise the information contained therein because of events and transactions occurring subsequent to the date of this report.

Independence

We are independent of Te Rua Mahara o te Kāwanatanga Archives New Zealand in accordance with the independence requirements of the Public Records Act 2005.

Contents

1. Executive summary

The Ministry of Defence (the Ministry) is the public service department responsible for advising the government on strategic defence policy, acquiring military equipment to meet defence capability, and conducting audits and assessments of the New Zealand Defence Force (NZDF).

The Ministry has a close partnership with NZDF who provides key services, including enterprise management systems, information communication technology (ICT) and general support. The Ministry's primary document management system is SharePoint. This is hosted by NZDF and has been used since 2017 to store records electronically.

The Ministry has approximately 150 full time staff. The Principal Information Advisor is a full time information management professional providing services to support the creation and management of information. The role is supported by the Executive Sponsor and managers who champion and promote information management in their teams. Most records are maintained electronically, with some non current hard copy files stored offsite at a commercial storage facility.

The Ministry's information management maturity is summarised below. Further detail on each of the maturity assessments can be found in Sections 4 and 5 of this report.

Beginning	**1**
Progressing	**4**
Managing	**6**
Maturing	**8**
Optimising	**1**

2. Introduction

KPMG was commissioned by Te Rua Mahara o te Kāwanatanga Archives New Zealand (Archives) to undertake an independent audit of the Ministry of Defence under section 33 of the Public Records Act 2005 (PRA). The audit took place in February 2023.

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

Archives provides the framework and specifies the audit plan and areas of focus for auditors. Archives also provides administrative support for the auditors as they undertake the independent component of the audit process. The auditors are primarily responsible for the onsite audit, assessing against the standard, and writing the audit report. Archives is responsible for following up on the report's recommendations with your organisation.

3. This audit

This audit covers all public records held by the Ministry, including both physical and digital information. While the NZDF also shares the same enterprise management systems, this audit is focused on the Ministry's information management practices.

The audit involved reviews of selected documentation, interviews with selected staff, including the Executive Sponsor, information management and technology staff, and a sample of other staff members from various areas of the Ministry. Note that the Executive Sponsor is the Senior Responsible Officer for the audit.

The audit reviewed the Ministry's information management practices against the PRA and the requirements in the Information Management and Records Standard and provides an assessment of current state maturity. As part of this audit, we completed systems assessments over the Ministry's key systems that act as a repository for public records. Where recommendations have been made, these are intended to strengthen the current state of maturity or to assist with moving to the next level of maturity.

The summary of maturity ratings can be found at Section 4, with detailed findings and recommendations following in Section 5. The Ministry has reviewed the draft report, and a summary of its comments can be found in Section 6.

4. Maturity Assessment

This section lists all assessed maturity levels by topic area in a table format, refer to Appendix 1 for an accessible description of the table. For further context about how each maturity level assessment has been made, refer to the relevant topic area in the report in Section 5.

Category	No.	Topic	Maturity				
			Beginning	Progressing	Managing	Maturing	Optimising
Governance							
	1	IM strategy				●	
	2	IM policy and processes				●	
	3	Governance arrangements & Executive Sponsor				●	
	4	IM Integration into business processes				●	
	5	Outsourced functions and collaborative arrangements		●			
	6	Te Tiriti o Waitangi		●			
Self-monitoring							
	7	Self-monitoring			●		
Capability							
	8	Capacity and capability				●	
	9	IM roles and responsibilities			●		
Creation							
	10	Creation and capture of information				●	
	11	High value / high-risk information		●			
Management							
	12	IM requirements built into technology systems			●		
	13	Integrity of information			●		
	14	Information maintenance and accessibility		●			
	15	Business continuity and recovery			●		
Storage							
	16	Appropriate storage arrangements					●
Access							
	18	Information access, use and sharing				●	
Disposal							
	20	Current organisation-specific disposal authorities				●	
	21	Implementation of disposal decisions			●		
	22	Transfer to Archives	●				

Please note: Topics 17 and 19 in the Information Management Maturity Assessment are applicable to local authorities only and have therefore not been assessed.

5. Audit findings by category and topic

Governance

The management of information is a discipline that needs to be owned from the top down within a public office. The topics covered in the governance category are those that need senior-level vision and support to ensure that government information is managed to ensure effective business outcomes for the public office, our government, and New Zealanders.

TOPIC 1 – IM Strategy — Maturing

Summary of findings

The Ministry has a comprehensive information management strategy that was approved by the Strategic Leadership Team (SLT) in 2021 and sets the direction of the information management workplan. The Ministry is planning a refresh of the strategy which expires in 2023 and is considering current plans and organisation-wide risks to further develop and improve the strategy.

Senior leaders actively support the implementation of the strategy and understand the importance of information management initiatives. However, due to a change in the Executive Sponsor (the Ministry appointed a temporary Executive Sponsor in November 2022, and will appoint a new Executive Sponsor in 2023) there has been a gap in ensuring the strategic direction of information management is being led in a consistent manner.

There is regular reporting on the five priorities identified in the strategy and on information management risks through quarterly reporting to the SLT. The SLT is provided with an annual information management update which includes a maturity self-assessment and priorities in the work programme for improving information management maturity.

Recommendation

Once a new Executive Sponsor is appointed, promote the information management strategic direction by communicating the strategy and associated workplan across the Ministry to ensure it is understood and implemented consistently.

TOPIC 2 – IM policy and processes — Maturing

Summary of findings

The Ministry has a current information management policy that was approved by the SLT in August 2022 and is consistent with the information management strategy and the PRA. The policy contains links to guidance documents, processes, and other relevant policies. The policy's requirements are built into most information systems and business processes, including the document management system. The NZDF Knowledge and Information Management Directorate (KIMD) site accessible to the Ministry, also contains documented information management processes for the document management system.

All staff and contractors are actively encouraged to meet their information management responsibilities through the onboarding programme they complete during their first two weeks at the Ministry. This includes an information management session which covers expectations and responsibilities and E-Learning provided by KIMD. Annual emails remind staff and contractors of the policy's guidance. Information management responsibilities have been added to all new staff and contractor job descriptions to encourage them to meet these responsibilities. However, information management responsibilities are not consistently addressed in the performance development plans of staff and contractors.

If a serious breach was identified, the Principal Information Advisor would escalate this immediately to the SLT. Due to the size of the organisation and close working relationship between the information management staff and senior leaders, all breaches are usually well communicated. For example, minor breaches with the security classification of information had been reported and managed at a senior leader level.

Recommendation

Include information management responsibilities in all staff and contractor's performance development plans.

TOPIC 3 – Governance arrangements and Executive Sponsor Maturing

Summary of findings

Due to the small size of the organisation, the Ministry's SLT is the information management governance group. The quarterly SLT reports and annual information management report supports information management strategic prioritisation, including resourcing. However, where any high-risk issues are identified, these are immediately reported to the SLT.

The Ministry has had changes in the Executive Sponsor role as outlined in *Topic 1 – IM Strategy*. The Executive Sponsor has fulfilled their oversight and monitoring role and actively promote the value and importance of information management. For example, the Executive Sponsor was instrumental in redrafting the information management policy and strategy so that it was fit for purpose. The Executive Sponsor has also promoted the importance of information management by establishing a champions network across all parts of the Ministry. However, due to the change in Executive Sponsor, the strategic direction has not been able to be led consistently as outlined in *Topic 1 – IM Strategy.*

The Executive Sponsor is part of the SLT and receives the quarterly and annual reports that are provided to the group. The Executive Sponsor also has bi-monthly meetings scheduled with the Principal Information Advisor to discuss the information management work programme and the status of current risks. Issues identified through this reporting and meetings are appropriately acted upon in a timely manner. The Executive Sponsor is not currently involved in any sector-wide information management networking groups.

Recommendation

Investigate opportunities for the new Executive Sponsor to network with other sector-wide information management networking groups.

TOPIC 4 – IM integration into business processes — Maturing

Summary of findings

Most of the Ministry's business processes and activities use the document management system which has information management requirements integrated into it. The document management system is divided into sites. Each site has a site manager that has completed specialist information management training to ensure information is managed correctly. For example, they are responsible for managing permissions and metadata on the site.

However, information management requirements are not integrated into all business processes and activities. Information management requirements are not integrated in the Capability Management Framework which guides how the Ministry manages large scale projects. The Ministry has added an item to its information management workplan and will address this gap within the next 12-18 months.

Information management staff are regularly involved in business process change and development. For example, information management staff were heavily involved in the recent development of the Crown Procurement site within the document management system to ensure information management requirements were understood and implemented. The use of site managers to manage smaller tasks means requests are usually responded to in a timely manner. It also allows the Principal Information Advisor to spend more time providing expertise on larger projects. The use of champions across the Ministry provides another resource for staff that require information management support with business processes and activities.

Recommendation

Integrate information management requirements into all business processes and activities.

TOPIC 5 – Outsourced functions and collaborative arrangements — Progressing

Summary of findings

The requirements for managing information are identified in some contracts for outsourced functions and collaborative arrangements. The Ministry outsources its payroll function to an external supplier and has identified some information management roles and responsibilities in this contract. The Ministry also has a Shared Service Agreement with NZDF. However, information management responsibilities are not clearly outlined in this agreement.

There is no regular monitoring to ensure information management requirements are met and issues addressed. However, an item would be added to the risk register if a significant risk was identified and would be monitored by the information management governance group. The Ministry advised Archives' guidance for outsourcing business functions will be implemented when the contracts are renewed.

Recommendation

Regularly monitor contracted parties to ensure information management requirements are being met. Include this in regular reporting to the information management governance group.

Where contracts are reviewed and renewed, ensure information management roles and requirements are defined.

TOPIC 6 – Te Tiriti of Waitangi — Progressing

Summary of findings

The Ministry is currently designing a process to identify information that is of importance to Māori, and this is supported by the organisation's Te Ao Māori strategy. The SLT has discussed how the Ministry can engage with Māori to gain their perspective on the information it may hold which is of value to them. The Ministry has also started identifying and adding information that is of interest to Māori into the Information Asset Register. However, the Ministry confirmed that it does not expect there to be a significant amount of information that is of interest to Māori or has treaty implications given the policy environment the Ministry works in.

Recommendation

Identify whether information held is of importance to Māori. Continue to document this within the Information Asset Register.

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 own internal policies and processes.

TOPIC 7 – Self-monitoring — Managing

Summary of findings

The Ministry regularly monitors its compliance with internal information management policies and processes. For example, major projects within the Ministry are monitored through Capability Project Boards. Compliance with PRA requirements, standards and other relevant legislation is monitored by using ComplyWith software during the annual audit.

Results of monitoring activities are reported to the SLT as outlined in *Topic 1 – IM Strategy.* Results of monitoring activities may also be reported to the Executive Sponsor during the bi-monthly meetings with the Principal Information Advisor.

Where monitoring actions identify any issues, these would be added to the information management risk register and corrective actions would be built into the work programme. For example, corrective actions were taken where information was found to be in an unusable format following the export of metadata out of the previous document management system. However, the implementation of some corrective actions on the information management work programme may not always be prioritised over other work.

Recommendation

Prioritise corrective actions based on the risk to information management and information management systems for the attention of the SLT.

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 **Maturing**

Summary of findings

The Executive Sponsor advised that the Ministry's capability and capacity is appropriately resourced to align to current and future business needs. The Ministry has a Principal Information Advisor who is dedicated to information management. Site owners for the document management system ensure the system is maintained and fit for purpose. There is another staff member in the Capability Delivery team who has an information management background and supports the embedding of information management processes across the Capability Project teams.

The Ministry is provided information management support from the NZDF as it uses shared platforms. KIMD provides advice on information management queries and manages the systems for the Ministry.

Consideration of the Ministry's information management capability and capacity is considered in workforce planning. For example, when the Principal Information Advisor was hired in 2022, the job description was reviewed at the same time and determined that the experience for the role needed to be at the principal rather than senior level. The job description for this role was reviewed and updated to meet information management requirements and business needs.

The Principal Information Advisor has the capacity to implement continuous improvement in information management practices including for example, by providing information management expertise in the development of the Departmental Procurement site. However, the Ministry's ability to implement information management improvements is limited as it is the responsibility of one full time staff member.

The Ministry prioritises improvements through a targeted information management work programme and considers additional resources for specific work programme items. For example, the Ministry has a standing arrangement with an information management practitioner who will provide mentoring and consultation during the refresh of the information management strategy.

All staff have regular access to broader professional development opportunities. For example, the Principal Information Advisor attended an external strategy course and has been involved in information management training courses provided by the NZDF. The Ministry is supportive and has encouraged information management staff to attend the training opportunities available to them.

Recommendations

Investigate whether the Ministry's capability and capacity is sufficient to sustain the implementation of continuous improvement in information management practices.

TOPIC 9 – IM roles and responsibilities Managing

Summary of findings

Information management roles and responsibilities are clearly communicated to all staff and contractors during the onboarding programme they complete in their first two weeks at the Ministry. This includes a series of meetings with staff across the Ministry, a mandatory thirty minute information management session and E-Learning provided by KIMD. However, completion of E-Learning modules is only monitored for Site Manager training. Targeted training is also available to staff and contractors in response to business needs and issues. This is communicated through team catch ups, and organisation wide emails.

Staff are also required to sign the Code of Conduct which outlines the expected behaviour of all staff. Information management responsibilities have recently been added to all job descriptions. However, a regular review process has not yet been established to ensure they remain aligned with the information management requirements and business needs.

Senior management understand their information management responsibilities and demonstrate good information management practice most of the time. The Ministry advised us that meeting minutes and business documents are usually filed correctly. However, there have been occasions where emails had not been filed correctly.

Recommendations

Monitor and enforce the completion of the mandatory information management module.

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 — Maturing

Summary of findings

Staff and contractors ensure the right information is created and captured as part of all business functions and activities within their unit. Most business processes are completed within the document management system and creating and capturing information correctly is embedded into the way staff and contractors work. Staff and contractors are required to apply metadata to the information they create to support the usability, reliability and trustworthiness of the information. System minimum metadata requirements are met.

Some staff noted that creating and capturing information was done differently across sites within the document management system. This made it difficult to assess whether information was reliable and trustworthy when using other sites. The Ministry provides some guidance on naming conventions. However, staff were not aware of this guidance and it was not well practiced across sites. Version creation is automated across the document management system.

The Ministry's systems are designed to ensure all information is managed in reliable and corporate-approved environments. For example, the system blocks USB sticks from extracting information.

Information is mostly considered to be reliable and trustworthy because its creation, use and management is well understood by staff and contractors. The Ministry's physical information and most of the digital information is considered reliable and trustworthy, with the exception of information extracted from some legacy systems. Information usability, reliability and trust issues are routinely monitored and reported on in the quarterly reporting to the SLT.

Recommendation

Remind staff of the standardised naming conventions across all sites within the document management system.

Assess the reliability and trustworthiness of information extracted from legacy systems.

TOPIC 11 – High-value / high-risk information

Progressing

Summary of findings

The Ministry has an inventory documenting all information held in all digital and physical systems. The Ministry has defined what sort of information would be high-risk and high-value and have begun developing an Information Asset Register. However, this is in the early stages and information assets currently held need to be formally identified. General risks to information and mitigations for these are identified in the Ministry's information management risk register, but not specifically for high-risk/high-value information.

Formally identifying high value/high-risk information is included in the Ministry’s information management work programme for the upcoming period.

Recommendation

Identify high-value/high-risk information assets.

Develop a plan to support the long-term management of high-value/high-risk information.

Management

Management of information should be designed into systems to ensure its ongoing management and access over time, including following a business disruption event. Information must be reliable, trustworthy and complete and managed to ensure it is easy to find, retrieve and use, as well as protected and secure.

TOPIC 12 – IM requirements built into technology systems

Managing

Summary of findings

Staff with information management expertise are involved in design, upgrade, commissioning and decommissioning of business systems. For example, NZDF is in the process of decommissioning the joint project management tool and they have reached out to the Ministry to ensure retention requirements are met under the Ministry’s disposal authority. The Principal Information Advisor, in their capacity as the information management lead, is working with NZDF to identify these requirements.

The Ministry and NZDF have ensured minimum metadata requirements are met for the document management system and will be for the upgrade of the document management system, as discussed in T*opic 10 – IM Requirements Built into Technology Systems*. System documents are maintained, and standardised information management practices are embedded into all business systems. For example, the document management system has been configured to enforce the user to structure content by sending links not attachments, automatically maintaining version control, and access only being granted by the site owner or manager.

The Ministry is supported by KIMD as well as NZDF's Defence Digital team to ensure upcoming and ongoing risks relating to business systems are mitigated. The Ministry engages with these teams for additional risk support.

Retention requirements are not built into information systems and the document management system does not have a retention schedule attached. Retention is maintained manually in a register. The Ministry and NZDF are implementing retention as part of the upgrade of the document management system and other business systems.

Recommendation

Implement disposal as part of the design and configuration of the upgraded document management system.

TOPIC 13 – Integrity of information — Managing

Summary of findings

The Ministry moved to a paperless operating model in 2018. Information is stored in the document management system, shared network drives, and specialised systems such as the invoice and reporting systems for finance information.

Information management practices are in place to ensure information is reliable and trustworthy. For example, Managers lead the use of the document management system by championing the information management in their unit, leading by example, and ensuring access is permitted where necessary.

The systems contain comprehensive metadata requirements, necessary use classifications and restricted access based on the type of work. The systems are backed up three times a week and this is managed by Defence Digital. Management controls are in place and regularly tested to maintain the integrity, accessibility, and usability of information. For example, staff can only access the file sites they are working on. Site owners have access to documents for their site, and the Principal Information Advisor holds a master copy of user access to all sites.

The Ministerial and Executive Services team responds to Archives' annual survey, confirming they have not had any issues locating information in the past year. The Ministry's intranet page contains guidance on information systems, storage locations for digital and physical information, and search techniques.

It was noted through focus groups that users occasionally have difficulty accessing information from different business units due to classification restrictions. NZDF and the Ministry have put document sharing controls in place to protect privacy and sensitive information. For example, documents cannot be shared over collaborative tools due to the classification of the information, and this makes collaborative working difficult.

Recommendation

Investigate better ways to document share and encourage collaborative working without compromising the integrity of information.

TOPIC 14 – Information maintenance and accessibility **Progressing**

Summary of findings

The Ministry has strategies in place to manage and maintain information during business and system changes. Physical information is stored in a single location with list registers and access control. Preservation for physical information has been identified and this includes the transfer of information to Archives. Risks to physical information are considered in the information management strategy and regularly assessed.

Digital information is largely managed by KIMD because they have a broader capability network than the Ministry. KIMD has been leading the Ministry through the upgrade of the document management system. The Ministry trusts digital risks and changes to be managed by NZDF and has established a collaborative relationship. For example, the Ministry’s Security Officer sits on the NZDF security board and represents the Ministry, as well as providing input into risk mitigation. Any risks identified would be communicated with the Ministry’s SLT and mitigated accordingly.

The Ministry does not have a digital strategy specific to their organisational needs, but are building towards this by identifying needs for digital preservation. Technology obsolescence risks are not identified for all digital information. The current systems do not support the transfer of information to Archives, and some information cannot be transferred because it cannot be declassified. The Ministry has a workplan to make a digital strategy and run a pilot to transfer to Archives. This includes identifying the type of information to be transferred and working with Archives to streamline this process.

Recommendation

Include a digital strategy for managing and maintaining digital information as part of the Ministry’s information management strategy.

TOPIC 15 – Business continuity and recovery **Managing**

Summary of findings

The Ministry has a business continuity and recovery plan which was last updated in February 2020. It covers the restoration of physical and digital information. The plan is split into phases and identifies scenarios, incidents, and examples of what is activated at each phase. Regular testing of the business continuity plan is undertaken by NZDF.

The Ministry is not involved in NZDF’s planning and prioritisation of business disruption events, particularly across digital information. The Ministry has little visibility over this process and while

NZDF systems are reliable, the Ministry needs to understand how well NZDF systems will protect its digital assets.

Digital restoration is further detailed in the Defence Force Instruction (DFI). This is owned, managed, and annually tested by NZDF. Due to the nature of shared systems, the instruction specifies the support services the Ministry receives from NZDF including facilities, security, communications, and infrastructure. Information management expertise from the Ministry is not involved in NZDF’s planning or prioritisation of what information is required following a business disruption event. In addition, the Ministry does not have visibility across testing conducted by NZDF.

Recommendation

Ensure the Ministry’s critical information and systems are identified in the business continuity plan managed by NZDF.

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

Optimising

Summary of findings

Digital information is stored on NZDF's secure infrastructure. The Ministry’s Chief Security Officer works with the Defence Cyber Security Centre to ensure information is protected from threat of compromise. Security reporting and information management reporting are included in the quarterly report to the SLT. This allows the SLT in their role as the information management governance group to monitor and oversee information management practices.

In the event of an incident, the Ministry would work with NZDF’s security incident response centre because NZDF have a larger capability network to support responses. If an instance of unauthorised access, information loss or deletion occurs, it is immediately reported to the Ministry's Executive Sponsor, who is also the Ministry's Chief Information Security Officer.

The Ministry's core digital information systems are securely stored on premise. The document management system is backed up three times a week and backups are deleted after five days.

Physical information of long-term importance is securely stored in an offsite storage facility and requires appropriate clearance to access this information. Physical information held in the office is limited and only accessible by people with the appropriate permissions.

Recommendation

The information management governance group should actively monitor and develop remediation actions for security risks.

Access

Ongoing access to and use of information enables staff to do their work and the public to hold government accountable. To facilitate this, public offices need mechanisms for finding and using this information efficiently. Information and/or data sharing between public offices and with external organisations should be documented in specific information sharing agreements.

TOPIC 18 – Information access, use and sharing

Maturing

Summary of findings

The Ministry actively maintains metadata schema to ensure the management and discovery of information is reliable. For example, project team members will request the incorporation of new metadata fields specific to their project.

Standard training of digital systems is provided to staff at induction and refreshed throughout the course of work. Site managers are given additional training so they can manage the use of metadata and access across the sites they are responsible for.

There is a template on how access permissions are managed within the document management system. Site security groups and access permissions are documented and maintained on an excel spreadsheet. Additionally, the document management system has controls that restrict access. Only site managers in each unit can add or remove members and this must be internally approved by site owners.

As noted in *Topic 13 - Integrity of information,* staff occasionally have difficulty accessing information from different business units due to clearance restrictions.

Recommendation

In conjunction with *Topic 13 - Integrity of information,* ensure access controls facilitate collaborative and transparent work practices.

Disposal

Disposal activity must be authorised by the Chief Archivist under the Public Records Act. 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 **Maturing**

Summary of findings

The Ministry has an organisation specific disposal authority that was approved in June 2021 and covers all formats. The Ministry has a disposal process that involves approval from the site owner and a tier three manager, as delegated by the Executive Sponsor.

The information management work programme includes annually reviewing the disposal authority to ensure it provides sufficient coverage and reflects business and legislative changes. Any changes to the functions of the Ministry are reported to SLT through information management quarterly reporting. If there is a functional change, this will be reviewed against the current disposal authority. The SLT champion good information practices and staff understand disposal requirements.

Recommendation

Actively monitor changes to legislation and reflect these in the annual review and update process.

TOPIC 21 – Implementation of disposal decisions **Managing**

Summary of findings

The Principal Information Advisor does an annual disposal of physical information at the offsite storage facility as approved by managers of the information. Disposal actions are fully documented in a disposal register and include the date of disposal, who carried it out, and the approval for action.

The document management system does not have the capability to automatically complete disposal, and this has to be processed and recorded manually. However, internal approvals to carry out disposal actions are routinely actioned.

Documents that are due for review and disposal still exist from the Ministry's previous document management system, Silent One. Files from the system are undergoing conversion to a readable format, and once this is complete, files will be reviewed for disposal. The upcoming upgrade of the document management system will support disposal and include this as a routine action.

Staff and contractors can find guidance on disposal policies and processes on the Ministry's intranet.

Recommendation

Review files and action disposal or retention from the previous document management system.

TOPIC 22 – Transfer to Archives Beginning

Summary of findings

Planning is underway to transfer physical information of archival value to Archives. The last transfer of physical information to Archives was done in 2014.

The Ministry's current systems do not support the transfer of digital information. As part of the work in retiring the previous document management system, Silent One, the Ministry plans to run a retention and disposal schedule over the digital information contained within it. The Ministry are planning to run a pilot digital transfer with Archives over the next year.

The Ministry needs to further identify information over 25 years old that is open or restricted access. There is no deferral agreement in place, but the Ministry has noted a need for this in the future.

Recommendation

Develop a deferral of transfer agreement for information that cannot be transferred to Archives New Zealand.

6. Summary of feedback

Manatū Kaupapa Waonga Ministry of Defence would like to thank KPMG and Archives New Zealand for the opportunity to participate in the Public Records Act 2005 Audit process.

The maturity assessment reflects the Ministry’s self-assessment and commitment to managing information in accordance with the Public Records Act 2005. We look forward to using the Audit Report to continue to improve the Ministry’s information management through our work programme.

7. Appendix 1

The table in Section 4, on page 3 lists all assessed maturity levels by topic area in a table format. This table has been listed below for accessibility purposes:

Topic 1, IM strategy – Maturing

Topic 2, IM policy and processes – Maturing

Topic 3, Governance arrangements & Executive Sponsor – Maturing

Topic 4, IM integration into business processes – Maturing

Topic 5, Outsourced functions and collaborative arrangements – Progressing

Topic 6, Te Tiriti o Waitangi – Progressing

Topic 7, Self-monitoring – Managing

Topic 8, Capability and capacity – Maturing

Topic 9, IM roles and responsibilities - Managing

Topic 10, Creation and capture of information – Maturing

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

Topic 12, IM requirements built into technology systems - Managing

Topic 13, Integrity of information - Managing

Topic 14, Information maintenance and accessibility - Progressing

Topic 15, Business continuity and recovery –Managing

Topic 16, Appropriate storage arrangements – Optimising

Topic 18, Information access, use and sharing – Maturing

Topic 20, Current organisation-specific disposal authorities – Maturing

Topic 21, Implementation of disposal decisions – Managing

Topic 22, Transfer to Archives – Beginning kpmg.com/nz

Te Rua Mahara o te Kāwanatanga
archives
NEW ZEALAND

2 August 2023

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

Andrew Bridgman
Chief Executive
Ministry of Defence
Andrew.bridgman@defence.govt.nz

Tēnā koe Andrew

Public Records Act 2005 Audit Recommendations

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

Introduction

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

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

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

Audit findings

In the audit report, the auditor has independently assessed your 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 Ministry’ IM practice is solidly at the Maturing and Managing maturity levels. This shows the high value that senior leadership gives to its information and the commitment (in collaboration with the New Zealand Defence Force) to its management.

The Ministry effectively distributes IM responsibility throughout the organisation to site owners who work with the Principal Information Advisor. With only one IM staff member this distributed model is useful in lessening risk, sharing the work as well as increasing IM knowledge across the organisation.

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 eight recommendations as identified in the Appendix.

What will happen next

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

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

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

Thank you again for your support with the audit. 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 noa, nā

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

Cc Mel Childs, Deputy Secretary, Governance People and Executive Services (Executive Sponsor), melanie.childs@defence.govt.nz

APPENDIX

Category	Topic Number	Auditor's Recommendation	Archive's Comments
Governance	5: Outsourced functions and collaborative arrangements	*Where contracts are reviewed and renewed, ensure information management roles and requirements are defined.*	For new and renewed contracts IM roles and requirements should be clearly identified and then monitored to ensure they are being met.
Governance	6: Te Tiriti o Waitangi	*Identify and assess whether information held is of importance to Māori. Continue to document this within the Information Asset Register.*	This is an uplift needed across the sector. From this work, the Ministry will directly benefit from increased understanding of its information and opportunities may present from this.
Capability	9: IM roles and responsibilities	*Monitor and enforce the completion of the mandatory information management module.*	This supports the understanding of IM across the organisation which is essential if a distributed model of delivery is used.
Creation	11: High-value/high-risk information	*Identify high/value/high-risk information.*	The identification of information assets and their value/risk to the organisation is useful in prioritising work with the information. This can be done leveraging off the development work for the organisation-specific disposal authority.
Management	12: IM requirements built into technology systems	*Implement disposal as part of the design and configuration of the upgraded document management system.*	This would align disposal consistently across physical and digital information.

Category	Topic Number	Auditor’s Recommendation	Archive’s Comments
Management	14: Information maintenance and accessibility	*Include a digital strategy for managing and maintaining digital information as part of the Ministry’s information management strategy.*	To ensure digital information continues to be accessible, digital continuity must be planned for including systems and formats.
Disposal	21: Implementation of disposal decisions	*Review files and action disposal or retention from the previous document management system.*	The improved functionality from the system upgrade will allow the Ministry to apply its disposal authority and benefit from the work in developing it.
Disposal	22: Transfer to Archives	*Develop a deferral of transfer agreement for information that cannot be transferred to Archives New Zealand.*	Discussion on physical (when possible) and digital transfers with Archives would be useful and agreement on the next steps, including the timing of development of any transfer deferral agreement.