



Public Records Audit Report for the New Zealand Productivity Commission

Prepared for Archives
New Zealand

December 2022



kpmg.com/nz

Disclaimers

Inherent Limitations

This report has been prepared in accordance with our Consultancy Services Order with 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 Archives New Zealand and the New Zealand Productivity Commission. 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 New Zealand Productivity Commission 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 Archives New Zealand and the New Zealand Productivity Commission'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 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 Archives New Zealand in accordance with the independence requirements of the Public Records Act 2005.

Contents

1. Executive summary	1
2. Introduction	2
3. This audit	2
4. Maturity Assessment	3
5. Audit findings by category and topic	4
Governance	4
Self monitoring	7
Capability	8
Creation	9
Management	10
Storage	12
Access	13
Disposal	14
6. Summary of feedback	17
7. Appendix 1	18



1. Executive summary

The New Zealand Productivity Commission (the Commission) is an independent Crown Entity that provides advice to the Government on improving productivity and the overall well being of New Zealanders. The Commission creates high value public records including research, data analysis, surveys, and commission reports.

The Commission has used SharePoint since 2015 as its primary document management system. Prior to that, digital information was stored on servers or hard drives. The Commission has desktop computers on premises called Datalabs with restricted access to designated staff. The desktop computers including the information stored in Datalabs are owned, managed and secured by Statistics New Zealand. There is minimal physical information created by the Commission as all information is digitised. Physical information is stored in a secured cabinet onsite. These documents are also digitised and saved on SharePoint

The Commission has approximately 20 full time equivalent staff members. Due to the size of the Commission, there is no dedicated information management staff member or governance group. Responsibilities for information management sit with the Director of Operations and Assurance Committee.

The Commission'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	6
Progressing	9
Managing	4
Maturing	0
Optimising	0

*Topic 22 Transfer to Archives New Zealand is not applicable



2. Introduction

KPMG was commissioned by Archives New Zealand to undertake an independent audit of the New Zealand Productivity Commission (the Commission) under section 33 of the Public Records Act 2005 (PRA). The audit took place in November 2022.

The Commission'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 New Zealand's Information Management Maturity Assessment.

Archives New Zealand provides the framework and specifies the audit plan and areas of focus for auditors. Archives New Zealand 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 New Zealand 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 New Zealand Productivity Commission including both physical and digital information.

The audit involved reviews of selected documentation, interviews with selected staff, including the Executive Sponsor, Information Management staff, the Information Technology team, and a sample of other staff members from various areas of the Commission. Note that the Executive Sponsor is the Senior Responsible Officer for the audit.

The audit reviewed the Commission's information management practices against the PRA and the requirements in the Information management and records standard and provides an assessment of the current maturity state. As part of this audit, we completed systems assessments over the Commission's key systems that act as repositories for public records. This includes SharePoint and emails. 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 Commission has reviewed the draft report, and a summary of their 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		●			
	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		●			
	10	Creation and capture of information		●			
	11	High-value / high-risk information	●				
	12	IM requirements built into technology systems			●		
	13	Integrity of information		●			
	14	Information maintenance and accessibility		●			
	15	Business continuity and recovery	●				
	16	Appropriate storage arrangements			●		
	18	Information access, use and sharing			●		
	20	Current organisation-specific disposal authorities	●				
	21	Implementation of disposal decisions	●				
	22	Transfer to Archives New Zealand	Not Applicable				

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

Progressing

Summary of findings

The Commission has an information management strategy, the *Information and Knowledge Management Strategy 2011*, that has been approved by senior management. However, the information management strategy was approved in 2011 and has not been reviewed since then. Additionally, the strategy is not used to direct information management initiatives and activities. For example, the strategy roadmap includes training to be provided to staff on the information management system, and staff members interviewed indicated not all of them have received such training.

The Commission plans to update its overall organisation strategy where information management is one of the focus areas. As part of this plan, the Commission is creating a new information management strategy which is aimed to be completed by early 2023. There is support for this plan from the Executive Sponsor and the Board.

Recommendations

Update the information strategy following guidance from Archives New Zealand and include an implementation roadmap in the strategy. This does not have to be a standalone strategy, as the Commission is a very small organisation, but should incorporate the key elements of information management.

TOPIC 2 – IM policy and processes

Progressing

Summary of findings

The Commission has two information management policies, *Using Information Systems Policy* and *Managing Information Policy*. These policies outline the organisation's requirements for using and managing information under the Public Records Act and other relevant legislation.

The Commission has identified that these policies require some updates. They were last approved in 2017 and 2019 respectively and do not include working from home protocol, disposal process and requirements, etc. Additionally, the Commission has identified that it does not have documentation available that details the process for creating, capturing and managing information.

Staff interviewed indicated that policies are not formally communicated across the organisation, and they are difficult to find on the intranet. Therefore, awareness of roles and responsibilities is limited to on-the-job training and information management requirements from their team leaders. The Commission intends to refresh its policies and establish the identified missing process documents alongside developing a new strategy to ensure there is widespread understanding of information management obligations under the PRA – see Topic 1 – *IM strategy*.

Recommendations

In connection with Topic 1 - *IM Strategy*, update the policies and ensure consistency with the information management strategy.

TOPIC 3 – Governance arrangements and Executive Sponsor

Progressing

Summary of findings

The Executive Sponsor understands and performs their oversight and monitoring roles at a strategic level. There are regular meetings on general operational matters between the Executive Sponsor and Director of Operations, who is the key information management resource. Information management issues are discussed during the meeting on an as-needed basis. Given there is no monitoring programme for information management, the Executive Sponsor's monitoring approach is reactive rather than planned and formalised.

The Assurance Committee is the governance group for information management. They receive quarterly updates from the Director of Operations on general operations where information management risks are identified and assessed in the risk management updates. However, the Assurance Committee responsibilities do not commonly cover day-to-day organisational operations and the Assurance Committee's Terms of Reference do not explicitly state what its information management responsibilities are.

Recommendations

In connection with Topic 1 – *IM strategy*, review the information management governance arrangement when developing the new information management strategy. Consider including information management responsibilities in the Assurance Committee's Terms of Reference or allocate the responsibilities to an appropriate governance group.

Summary of findings

Requirements for managing information are integrated in the Commission’s business processes. Information management is integrated into day-to-day activities where staff collaborate by sharing information and working on documents through SharePoint.

Information management responsibilities for business owners are documented in the information management policies (refer to Topic 2 – *IM Policy and Processes*). However, the responsibilities and policies are not communicated to staff and contractors. Staff and contractors are assigned information management responsibilities through day-to-day activities by their team leaders, such as saving documents in the correct folders.

Recommendation

Communicate information management responsibilities through induction training and raise awareness of the relevant policies on the intranet.

Summary of findings

Requirements for managing information are outlined in some but not all contracts where there are outsourced functions or collaborative arrangements. For instance, one contract reviewed used a third-party contract template and specified the contracted party’s information management obligations such as returning information on termination. The contract also recognised the status of the documents handled as public records. However, the Commission’s standard contract template does not include requirements for managing information or acknowledging the public record status of records created.

There is limited evidence of monitoring contracted parties to ensure information management requirements are met. For example, team leaders ensure all information and documents have been filed appropriately before the contractors’ departure.

Recommendation

Update the Commission’s contract template and ensure all contracts, outsourced functions and collaborative arrangements that involve public records include information management requirements.

Summary of findings

The Commission has not identified any information they hold of importance to Māori, nor have they reviewed the information management implications of Te Tiriti o Waitangi in relation to the

information that the Commission creates. The Commission indicated it would like to progress in this area and wants to understand its obligations under Te Tiriti.

Recommendations

Undertake consultation with Māori groups and iwi expertise to identify and document information of importance to Māori.

Self-monitoring



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

TOPIC 7 – Self-monitoring

Progressing

Summary of findings

The Assurance Committee receives quarterly updates from the Director of Operations on internal control activities and risk management. Those quarterly updates cover some information management topics such as information security, information retention, etc. However, there is no regular or formal monitoring of information management compliance against the Commission's internal policies. Issues around information management are discussed with the Assurance Committee when identified.

The Assurance Committee and Director of Operations work together and complete an annual Legislative Compliance Report to monitor compliance with PRA requirements and other legislative standards. Where opportunities for improvement are identified, the Director of Operations will discuss these with the Assurance Committee. Remediation actions are approved by the Board.

Recommendation

Establish a regular and proactive approach to monitor compliance with internal policies and the Public Records Act.



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

Managing

Summary of findings

Due to the size of the organisation, the Commission has no dedicated personnel for information management. The Executive Sponsor and Director of Operations indicated the Commission's information management capacity and capability are appropriate for their organisational needs. If an increase in capability was needed to improve information management maturity, the Commission indicated this would be resourced through external parties or contractors.

Staff who is responsible for information management do not receive dedicated information management training however, they can request professional development in information management.

While business needs are currently met, information management capacity and capability are not regularly monitored or assessed. This is in part due to the absence of an up-to-date information management strategy and a lack of monitoring against policies.

Recommendation

In connection with Topic 1 – *IM strategy*, formally assess capacity and capability for information management against business needs when reviewing information management strategy.

TOPIC 9 – IM roles and responsibilities

Progressing

Summary of findings

Staff interviewed indicated some awareness of their information management responsibilities. There is no formal induction or regular information management training. Staff learn information management responsibilities through informal on-the-job training, and guidance from their team leaders. While information management practices are functional, they could be improved to standardise information management practise across the Commission. Staff interviewed also indicated a lack of understanding of information management responsibilities of team leaders.

While the Code of Conduct acknowledges employee's information management obligations, roles and responsibilities specific to information management are not documented in job descriptions or performance plans. The Director of Operations has identified the need for information management training, especially focusing on the disposal of information.

Recommendations

Include information management responsibilities in staff job descriptions.

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

Progressing

Summary of findings

Staff at the Commission indicated they understand and comply with their obligations to create full and accurate records through informal on-the-job training and guidance from their team leaders. Information is routinely created and captured as part of all business functions and activities. Staff understand how to create and capture information to ensure it is usable, reliable, and that complete records are maintained. For example, staff are required to save the data sources used in research reports in SharePoint so the research results can be traced back.

Information is managed in the controlled environment of SharePoint with appropriate metadata to support the usability, reliability and trustworthiness of the information. Staff can use OneDrive to capture some work-in-progress documents. However, given many records require collaboration and wider access, individual environments are discouraged.

There is no monitoring programme for information management (refer to Topic 7 – *Self-monitoring*), and therefore there is no structured approach to monitor information usability, reliability and trust issues by the Commission.

Recommendation

In conjunction with Topic 7 – *Self-monitoring*, include monitoring the creation and capture of information when developing the monitoring approach.

TOPIC 11 – High-value / high-risk information

Beginning

Summary of findings

The Commission indicated it does not hold or store any information that is of high-risk. This is because most of the information the Commission holds is either publicly available or owned by a separate organisation. For example, the information in Datalabs is owned, managed and

secured by Statistics New Zealand (Stats NZ). Staff follow Stats NZ's protocols in using these data.

The Commission has not identified any high risk or high-value information. As a result, there is no management plan for information that may be considered high-value. An inventory list is not maintained for information held in digital and physical systems.

Recommendation

Develop an information asset register that identifies information held by the Commission that is high-value or high-risk. If the Commission holds any private information, this should be included as 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

Third-party IT providers manage and deliver the Commission's technology systems. The Director of Operations works with the third-party providers to ensure technology systems are up to date. Due to the lack of a current information management strategy, information management requirements are defined on a case-by-case basis if a system was to be upgraded, commissioned, or decommissioned. For example, the onsite server will be decommissioned in 2023, therefore the Commission has transformed all systems and information to be cloud-based.

Documentation is maintained for SharePoint by third-party IT providers, and this includes system design, configuration, and architecture.

While SharePoint meets minimum metadata requirements, staff noted inconsistent naming conventions made it difficult to locate documents at times.

Recommendation

Ensure there are metadata and disposal requirements and processes to facilitate the retention of information of long-term value.

Summary of findings

Team members have confidence that information is reliable and trustworthy. Raw data used in research is taken from public surveys, or from external sources like Stats NZ. Documents are saved on SharePoint and this keeps track of version history, data sources, file creators, and other metadata. In addition, published or finalised documents are locked so they cannot be edited.

Staff and contractors are aware that the information they create and manage should be comprehensive and complete. However, this awareness is based on individual team leaders' expectations, and on-the-job training, leading to varied practices across the organisation.

Staff and contractors have varied experiences when trying to find and retrieve information. This difficulty is primarily due to inconsistent naming conventions across SharePoint, as noted in Topic 12 – *IM requirements built into technology systems*.

Recommendations

Identify the integrity issues that staff have around finding, retrieving and using information across the organisation and develop a plan to address these.

Summary of findings

Digital systems are managed by third-party IT providers. Technology risks are monitored by the Director of Operations and third-party IT providers. All software and tools are up-to-date, and the only technology at risk of obsolescence is the onsite server. All information from the server has been transferred to SharePoint and the server will be removed in 2023.

There is a single filing cabinet onsite which holds human resource records, credit card statements and invoices. This information is also stored electronically. The cabinet is locked, and only designated staff have the key to access it.

Digital information is stored in the cloud and backed up daily. All staff have their own laptops, IT equipment, and capability to work remotely or from the office. This means staff are equipped to work effectively during business changes. Any system changes like updates, would be communicated to staff and supported by the third-party IT providers. However, there are no strategies for the management and maintenance of information during business and system changes.

Recommendations

Develop strategies for management and maintenance of digital information and ensure these are part of the planning for any business and system change.

Summary of findings

The Commission has a business continuity plan which was last updated in 2016 and approved by management. This was written by the third-party IT provider and outlines digital information recovery, salvage and restoration. However, the plan is not regularly tested, and needs to be updated to reflect the current operations of the entity, such as working remotely, and digital functions now being cloud-based.

Recommendations

Update the business continuity and recovery plan and ensure critical information is identified.

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.

Summary of findings

There is appropriate protection and security to protect physical information against unauthorised access, loss, or destruction. Access to the office is via swipe card and access to Datalabs is restricted to certain staff who require an access code. Stats NZ checks and resets the Datalabs security code quarterly. Within the office, physical information is stored in a locked filing cabinet. Only designated staff are issued the key to access the cabinet. All physical information is also saved electronically with restricted access set up in SharePoint to authorised staff.

Digital information is saved on the cloud-based SharePoint. The Commission has enforced multi-factor authentication for remote access. Protection and security processes are tested regularly by third-party providers, and an annual cyber security report is provided to the Executive Sponsor. Additionally, information protection and security risks are reported to the Information Management Governance Group quarterly.

However, given there is no information management specific training, not all staff and contractors are aware of the protection and security risks for managing information.

Recommendations

In connection with Topic 4 - *IM integration into business processes*, support all staff and contractors to understand the protection and security requirements for information management.



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

Managing

Summary of findings

SharePoint enables the application of metadata to facilitate the management and discovery of information. SharePoint automatically captures the minimum required metadata. However, staff noted naming conventions could be applied more consistently so it is easier to find and locate documents on SharePoint.

Access controls to information are maintained by the third-party IT provider and monitored by the Director of Operations. For example, any new access to SharePoint requires approval from the Director of Operations. The Director of Operations reviews the user access report semi-annually. Staff and contractors know how to use SharePoint to find information as the folder structure in SharePoint is standardised.

Recommendations

Assess the need for advanced training on standardised name conventions and search techniques.

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 New Zealand (or have a deferral of transfer) and be determined as either “open access” or “restricted access”.

TOPIC 20 – Current organisation-specific disposal authorities

Beginning

Summary of findings

The Commission does not have an organisation-specific disposal authority. The Commission has been in existence for 11 years and all records have been retained throughout this time except financial records, which are disposed after seven years by their third-party financial management provider with approval from the Director of Operations. The disposal of financial records is authorised under General Disposal Authorities 6 (GDA6).

The Commission intends to develop an organisation-specific disposal authority.

Recommendations

Develop an organisation-specific disposal authority which covers all information and business functions and obtain approval from Archives New Zealand.

TOPIC 21 – Implementation of disposal decisions

Beginning

Summary of findings

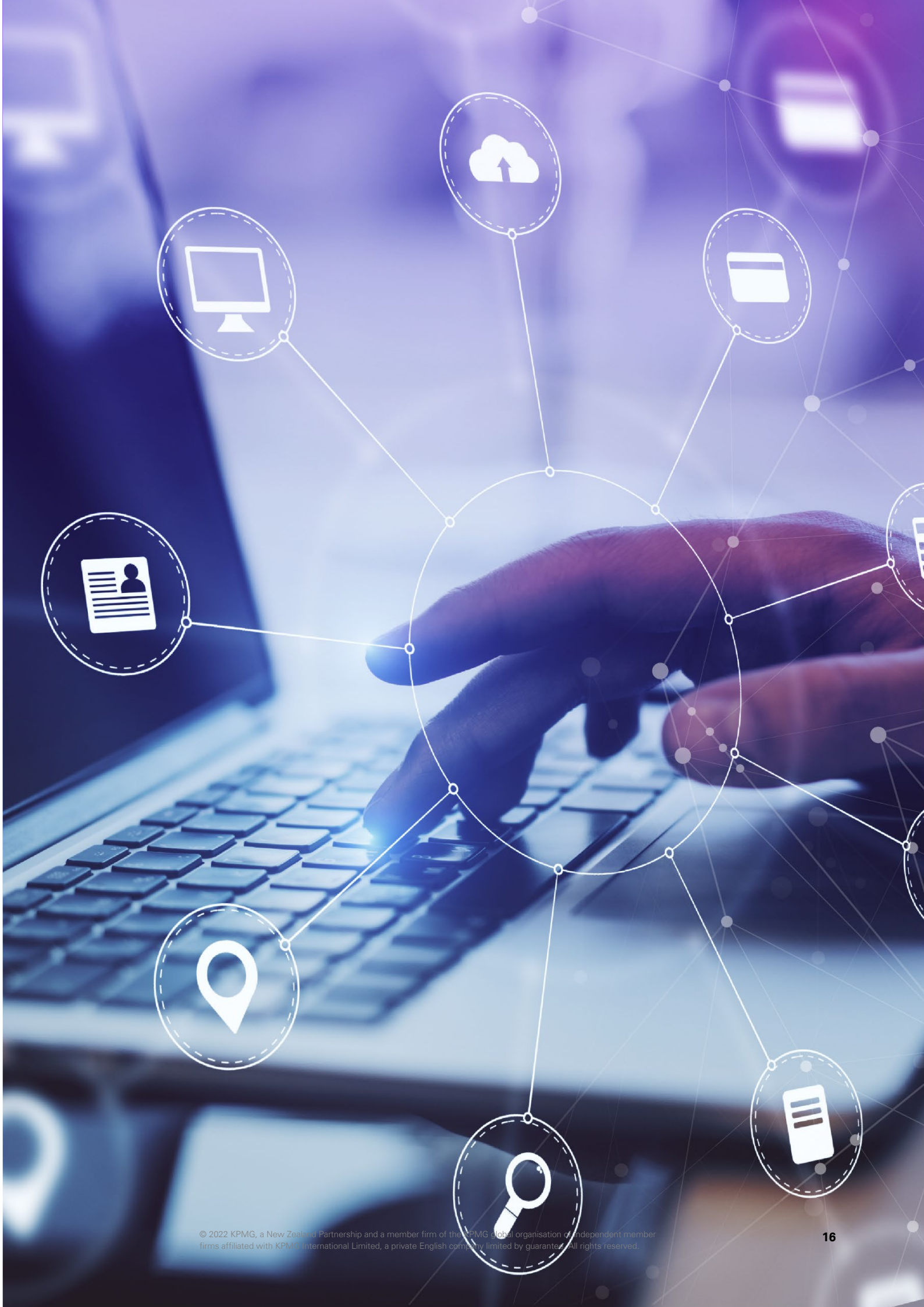
As stated in Topic 20 – *Current organisation-specific disposal authorities*, all information (except for financial records) has been retained since the establishment of the Commission. There is no process to identify information for disposal.

Recommendations

Develop a disposal plan against General Disposal Authorities and routinely carry out disposal actions for physical and digital information.

Summary of findings

The Commission was established in 2011 and therefore does not have any information that is over 25 years old. We have not provided an assessment for this topic.



6. Summary of feedback

The Commission found that the Maturity Assessment and subsequent recommendations made in the audit report were in line with the Commission's self-assessment and so there were no surprises. The Commission intends to be able to implement recommendations almost immediately.

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 – Progressing

Topic 2, IM Policy – Progressing

Topic 3, Governance arrangements & Executive Sponsor – Progressing

Topic 4, IM integration into business processes – Progressing

Topic 5, Outsourced functions and collaborative arrangements – Beginning

Topic 6, Te Tiriti o Waitangi – Beginning

Topic 7, Self-monitoring – Progressing

Topic 8, Capability and capacity - Managing

Topic 9, IM roles and responsibilities - Progressing

Topic 10, Creation and capture of information - Progressing

Topic 11, High-value / high-risk information – Beginning

Topic 12, IM requirements built into technology systems - Managing

Topic 13, Integrity of information - Progressing

Topic 14, Information maintenance and accessibility - Progressing

Topic 15, Business continuity and recovery – Beginning

Topic 16, Appropriate storage arrangements – Managing

Topic 18, Information access, use and sharing – Managing

Topic 20, Current organisation-specific disposal authorities – Beginning

Topic 21, Implementation of disposal decisions – Beginning

Topic 22, Transfer to Archives New Zealand – Not applicable

kpmg.com/nz



09/03/2023

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

Ganesh Nana
Chair
New Zealand Productivity Commission
ganesh.nana@productivity.govt.nz

Tēnā koe Ganesh

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the New Zealand Productivity Commission 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.

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 Archives' mandatory Information and records management standard.

The Commission's IM is assessed as operating mostly at the 'Progressing' maturity level with a significant amount still at 'Beginning'. A small organisation is not expected to have in-house IM staff but external IM expertise is needed to work with the third-party IT provider and with staff to increase maturity in some areas. The Commission is well positioned to increase its IM maturity with its implementation of SharePoint.

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 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
Chief Archivist

Te Rua Mahara o te Kāwanatanga Archives New Zealand

Cc The Chair is also the Executive Sponsor

APPENDIX

Category	Topic Number	Auditor's Recommendation	Archive's Comments
Governance	1: IM strategy	<i>Update the information strategy following guidance from Archives New Zealand and include an implementation roadmap in the strategy. This does not have to be a standalone strategy, as the Commission is a very small organisation, but should incorporate the key elements of information management.</i>	It would be useful to the Commission to have some priorities to direct their activity and to understand the IM resourcing requirements of a roadmap to implement activities.
Governance	2: IM policy and processes	<i>In connection with Topic 1 – IM Strategy, update the policies and ensure consistency with the information management strategy.</i>	Up-to-date and well-communicated IM policies and procedures will help staff understand what is required of them to fulfil their IM responsibilities.
Governance	5: Outsourced functions and collaborative arrangements	<i>Update the Commission's contract template and ensure that all contracts, outsourced functions and collaborative arrangements that involve public records include information management requirements.</i>	Once this is done the requirements should be monitored to ensure they are met.
Capability	10 Creation and capture of information	<i>In conjunction with Topic 7 – Self-monitoring, include monitoring the creation and capture of information when developing the monitoring approach.</i>	Decide what aspects of IM should be monitored, for instance high-value information, and what reporting should be produced to give the organisation confidence that information is well managed.
Creation	11: High-value/high-risk information	<i>Develop an information asset register that identifies information held by the Commission that is high-value or high-risk. If the Commission holds any private information, this should be included as high-risk information.</i>	Understanding the information that you create and manage is essential in prioritising your IM and should be done in conjunction with or lead to the development of an organisation-specific disposal authority. IM expertise will be needed for this work.

Category	Topic Number	Auditor's Recommendation	Archive's Comments
Management	13: Integrity of information	<i>Identify the integrity issues that staff have around finding, retrieving and using information across the organisation and develop a plan to address these.</i>	Some work is needed to identify issues for staff in using and finding information in SharePoint. Specialist IM help may be needed to assist with this, as well as to develop induction and/or refresher training to establish good IM practice across the organisation.
Management	15: Business continuity and recovery	<i>Update the business continuity and recovery plan and ensure critical information is identified.</i>	Identification of critical information can be done in conjunction with the work recommended in Topic 4: <i>High-value/high-risk.</i>