



# Public Records Audit Report for National Pacific Media Trust

Prepared for Te Rua Mahara o te Kāwanatanga Archives  
New Zealand

December 2023



## **Disclaimers**

### **Inherent Limitations**

This report has been prepared and is delivered by KPMG, a New Zealand partnership (KPMG, we, us, our) subject to the agreed written terms of KPMG's CSO with the Department of Internal Affairs (Client, you) dated 26 November 2020 (Engagement Contract).

Unless stated otherwise in the Engagement Contract, this report is not to be shared with third parties without KPMG's prior written consent. However, we are aware that you may wish to disclose to the National Pacific Media Trust elements of any report we provide to you under the terms of this engagement. In this event, we will not require the National Pacific Media Trust to sign any separate waivers.

The services provided under our Engagement Contract (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/information provided by the Department of Internal Affairs and the National Pacific Media Trust. 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. Nothing in this report constitutes legal advice or legal due diligence and you should not act upon any such information without seeking independent legal advice.

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 National Pacific Media Trust management and personnel / stakeholders consulted as part of the process.

This report was based on information available at the time it was prepared. KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form.

### **Third Party Reliance**

This report is solely for the purpose set out in Section 2 and 3 of this report and for the Department of Internal Affairs 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 the Department of Internal Affairs, none of KPMG, any entities directly or indirectly controlled by KPMG, or any of their respective members or employees assume 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 (Te Rua Mahara) in accordance with the independence requirements of the Public Records Act (PRA) 2005.

# Contents

<b>1. Executive summary</b>	<b>1</b>
<b>2. Introduction</b>	<b>2</b>
<b>3. This audit</b>	<b>2</b>
<b>4. Maturity Assessment</b>	<b>3</b>
<b>5. Audit findings by category and topic</b>	<b>4</b>
Governance	4
Self monitoring	6
Capability	7
Creation	8
Management	9
Storage	11
Access	12
Disposal	13
<b>6. Summary of feedback</b>	<b>16</b>
<b>7. Appendix 1</b>	<b>17</b>



# 1. Executive summary

The National Pacific Media Trust (NPMT) was established in 2002 through a trust deed with the Government. The delivery entity, Pacific Media Network (PMN), is a public interest broadcaster for Pacific peoples in New Zealand. PMN operates two national radio networks, NiuFM and 531pi, offering radio programmes in 10 Pacific languages. PMN aims to empower, encourage, and nurture cultural identity and economic prosperity by delivering the best in Pacific content.

NPMT creates and maintains public records in relation to:

- Information on programmes and services
- Information on operating leases and financial documents
- Recorded/filmed and archived Pacific content delivered on air and online.

NPMT maintains its information on shared drives and several business systems, including a payroll, radio scheduling and playout, and financial management system.

NPMT employs 45 full time staff and follows a decentralised approach to information management. Responsibility for information management is delegated to NPMT's various business units. There is an Information Technology (IT) Manager, but no dedicated Information Manager at NPMT.

NPMT maintains information in physical and digital formats. Physical information, such as financial records, is stored onsite. The majority of digital information is kept on a server, with backup discs also located onsite.

NPMT'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.

<b>Beginning</b>	<b>14</b>
<b>Progressing</b>	<b>5</b>
<b>Managing</b>	<b>0</b>
<b>Maturing</b>	<b>0</b>
<b>Optimising</b>	<b>0</b>
<b>Not applicable</b>	<b>1</b>



## 2. Introduction

KPMG was commissioned by Te Rua Mahara o te Kāwanatanga Archives New Zealand (Te Rua Mahara) to undertake an independent audit of the NPMT under section 33 of the PRA. The audit took place in November 2023.

NPMT's information management (IM) practices were audited against the PRA and the requirements in the [Information and records management standard](#) (the Standard) as set out in the Te Rua Mahara Information Management Maturity Assessment.

Te Rua Mahara provides the framework and specifies the audit plan and areas of focus for auditors. Te Rua Mahara 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 and writing the audit report. Te Rua Mahara is responsible for following up on the report's recommendations with your organisation.

## 3. This audit

This audit covers all public records held by NPMT including both physical and digital information.

The audit involved the review of selected documentation, interviews with selected staff, including the Executive Sponsor, IM staff, the information technology team, and a sample of other NPMT staff. The Executive Sponsor is the Senior Responsible Officer for the audit.

The audit reviewed NPMT IM practices against the PRA and the requirements in the Standard and provides an assessment of current state maturity. As part of this audit, we completed systems assessments over NPMT's key systems that act as a repository for public records. The systems assessed were NPMT's shared network drives, emails, and radio playout system. 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. NPMT 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
<b>Governance</b>							
	1	IM strategy	●				
	2	IM policy and processes	●				
	3	Governance arrangements and Executive Sponsor		●			
	4	IM Integration into business processes	●				
	5	Outsourced functions and collaborative arrangements	●				
	6	Te Tiriti o Waitangi		●			
<b>Self-monitoring</b>							
	7	Self-monitoring	●				
<b>Capability</b>							
	8	Capacity and capability	●				
	9	IM roles and responsibilities	●				
<b>Creation</b>							
	10	Creation and capture of information	●				
	11	High-value / high-risk information		●			
<b>Management</b>							
	12	IM requirements built into technology systems	●				
	13	Integrity of information		●			
	14	Information maintenance and accessibility	●				
	15	Business continuity and recovery	●				
<b>Storage</b>							
	16	Appropriate storage arrangements		●			
<b>Access</b>							
	18	Information access, use and sharing	●				
<b>Disposal</b>							
	20	Current organisation-specific disposal authorities	●				
	21	Implementation of disposal decisions	●				
	22	Transfer to Te Rua Mahara					N/A

**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

Beginning

#### *Summary of findings*

NPMT does not have an IM Strategy in place to provide direction and support for information management activities within the organisation.

The Executive Sponsor is new to the role and showed an awareness of the need to incorporate IM into the organisation's overall strategic direction. NPMT has invested in information technology (IT) improvements, such as a new human resources (HR) management system.

#### *Recommendation*

Develop an IM Strategy or integrate one within a related strategic document following guidance from Te Rua Mahara. The Strategy should be approved by senior management, communicated to all staff and contractors, and reviewed on a periodic basis to ensure it continues to support NPMT's business needs and the strategic direction of the organisation.

### TOPIC 2 – IM policy and processes

Beginning

#### *Summary of findings*

There is no current IM Policy or associated processes in place. Roles and responsibilities for IM have not been identified and staff do not have guidance on IM practices. As a result, staff do not have consistent awareness of their roles and responsibilities for IM.

The lack of an IM Policy and associated processes has led to an inconsistent approach to IM across NPMT, contributing to IM issues experienced by staff, such as difficulty accessing non-current archives for Pacific media content.

The Executive Sponsor noted that the organisation is planning to develop a data management policy which will formally document IM roles and responsibilities. Work to develop this has not yet commenced.

### ***Recommendation***

Develop an IM Policy, and associated processes and guidance in consultation with staff. Communicate these throughout the organisation.

---

## **TOPIC 3 – Governance arrangements and Executive Sponsor**

**Progressing**

### ***Summary of findings***

The Technology Committee is the governance group responsible for IM matters, which includes the Executive Sponsor and the IT Manager. The Executive Sponsor is the CEO and understands the importance of their oversight and monitoring role. IM concerns and developments are reported to the Technology Committee by its members as needed. Regular reporting of IM activity to the Technology Committee, such as compliance with IM requirements, is yet to be formalised.

The Technology Committee was recently established, and the Terms of Reference are still being developed.

### ***Recommendations***

Design and implement regular IM reporting that provides useful and actionable information to the Executive Sponsor and the Technology Committee.

---

## **TOPIC 4 – IM integration into business processes**

**Beginning**

### ***Summary of findings***

IM responsibilities have not been formally assigned to staff due to the absence of an IM Strategy, Policy, and associated processes. IM roles, responsibilities and requirements are not clearly integrated into business processes and activities across the organisation as they have only been identified in a small number of processes, such as the end-to-end receivables process. As a result, IM practices at NPMT are inconsistent, and vary depending on the practices of each business unit.

Expectations for some aspects of IM are communicated to staff. However, IM requirements are not consistently identified or are only communicated at a high level. For example, the IT Manager said there is an expectation that corporate records are stored on a shared network drive, but there is no guidance on where these should be stored on the drive to enable ongoing accessibility.

### ***Recommendation***

Assess requirements for managing information created by the business processes. Ensure IM responsibility is assigned to business owners.



### ***Summary of findings***

Requirements for managing information are included in some, but not all, contracts where there are outsourced functions or collaborative arrangements. For example, a contract for transmission management specifies that NPMT retains ownership and copyright of the information it creates. However, another contract relating to a collaborative arrangement for content sharing did not identify any IM requirements.

IM roles and responsibilities are identified in some, but not all, contracts for outsourced functions or collaborative arrangements. For example, one contract required the third party to ensure that information was handled appropriately to maintain confidentiality, but the second contract did not identify any IM roles and responsibilities.

There was no evidence of monitoring contracted parties to ensure IM requirements were met.

### ***Recommendations***

Ensure that IM requirements are identified when creating contracts for outsourced functions and collaborative agreements where public records are created and managed.

### ***Summary of findings***

The Executive Sponsor confirmed that the organisation holds information that is important to Māori as it has an agreement with a third-party to promote Māori language radio. There is no documented guidance on how this information should be classified, despite the use of manual metadata tags to identify Māori audio in the radio playout system.

Staff have a good understanding of NPMT's agreements with Māori, but the IM implications of these agreements are not well understood.

### ***Recommendation***

Establish IM processes to identify information of importance to Māori, considering the role of NPMT as a public interest broadcaster.

## 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.

***Summary of findings***

There is no regular monitoring of IM practices, due to there being no established Policy or processes in place. Instead, monitoring of IM happens within business units on an ad-hoc basis.

***Recommendation***

Identify IM activities to be monitored and implement.

**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.

***Summary of findings***

There is limited capacity for NPMT to work on, and drive, IM activities. The Executive Sponsor takes on IM duties for NPMT but is new to their role. The Executive Sponsor has a wide range of duties and due to the daily demands on their position they have limited capacity to work on IM activities. There is limited IM expertise within the organisation.

Based on the overall IM maturity of NPMT, there are significant capacity and capability requirements to be addressed. NPMT acknowledges this and is aware of the lack of capacity and capability.

***Recommendation***

Assess NPMT's IM capacity and capability against business needs and plan to address these internally or with external assistance.

***Summary of findings***

NPMT staff have limited awareness of their IM responsibilities. Because IM policies and processes are not yet documented, staff understanding of IM is inconsistent and relies on personal experience.

Three job descriptions were sampled as part of this audit. Only one of these descriptions included specific IM responsibilities. None referenced the PRA.

Staff members have not received formal induction or ongoing training on IM. Instead, IM training is primarily delivered in response to changes in business systems, such as the radio playout system. Staff raised that some of these training sessions do not include all relevant staff members.

***Recommendation***

Assess the need for IM training during induction and ongoing. Design and implement the training.

**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.

***Summary of findings***

Staff and contractors are not well supported to understand their obligation to create and capture full and accurate records, due to the lack of training and guidance. Information is routinely created and captured as part of some, but not all, business functions and activities. For example, information relating to HR is routinely captured in the HR management system. However, information relating to programme content is not consistently created and captured.

NPMT uses shared network drives, and staff can use personal external drives on all organisation computers except those located in broadcasting studios. Personal drives are uncontrolled. There is no monitoring of what information is created and saved on these drives. There is no formal and documented guidance to discourage the use of uncontrolled environments.

### **Recommendation**

Include in the IM Policy the requirement for staff to use organisation's systems and monitor this.

## **TOPIC 11 – High-value / high-risk information**

**Progressing**

### **Summary of findings**

There is no formalised approach to identify high-value or high-risk information assets held by NPMT. There is some understanding of what is considered high-risk or high-value information, for example, staff recognise that the Storage Area Network (SAN) data storage system holds the majority of the organisation's critical data, while the PMN website contains high-value historical articles. The IT Manager has developed a list of some high-value and high-risk digital information. However, this is not complete and has not been formally endorsed by the Technology Committee.

### **Recommendation**

Develop and maintain an information asset register which covers both digital and physical information, and identifies all information assets that are high-value or high-risk.

## **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**

**Beginning**

### **Summary of findings**

IM expertise is not regularly involved in the design and configuration of new and upgraded business systems. External IM expertise is engaged on an ad-hoc basis as there is a lack of internal IM expertise.

No standardised IM requirements are used to inform the implementation or upgrading of systems. There is no standardised process to ensure that the minimum metadata requirements specified by Te Rua Mahara are incorporated into the design and implementation of new or upgraded business systems.

### ***Recommendation***

Create standardised IM requirements for new and upgraded business systems and ensure that IM expertise is included as part of the system change process. The requirements should specify the minimum metadata requirements needed to align with the Standard.

## **TOPIC 13 – Integrity of information**

**Progressing**

### ***Summary***

Staff interviewed largely understood their responsibilities to create information that is comprehensive and complete. Staff noted some localised IM practices across business units which are not documented. For example, there is an understanding among staff that file version numbers should be used to differentiate between different versions of the same document.

Staff shared they had variable experiences when trying to find and retrieve information, but they are typically aware of the records their teams create. When staff require information from other business units, the inconsistent IM approaches can slow the process of accessing required files and staff are often reliant on their colleagues to source the information. For example, there is no consistent approach to filing documents in the shared network drive which makes it difficult to locate various kinds of records across NPMT.

### ***Recommendation***

Develop and socialise a process for the shared drive that ensures consistent practice across the organisation.

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

**Beginning**

### ***Summary of findings***

There are no documented strategies in place to manage and maintain physical information during business and system change projects. Staff reported the loss of the audio recordings of almost a year's worth of radio broadcasts due to a technical error during a system change.

NPMT has identified several technology obsolescence risks, such as the use of an outdated operating system on two computers and storage capacity issues. The organisation does not delete information, and there is a strong reliance on backups to protect digital information. There is currently no plan to address this, but the IT Manager has identified several options, one of which includes using cloud storage.

The ongoing accessibility risks associated with physical information have not been documented, identified, or addressed. For instance, physical information stored onsite lacks adequate labelling. Preservation needs for physical information are inconsistently identified and addressed. While there was a digitisation project for financial records, requirements for digitising other corporate records have not been identified.

### ***Recommendation***

Assess risks to the ongoing accessibility of digital and physical information and plan to address the risks.

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

**Beginning**

### ***Summary of findings***

NPMT does not currently have a business continuity and recovery plan in place, although there is a draft Disaster Management Policy. As a result, critical information that would need restoration following a business disruption event has not been identified. However, backups of digital information can be accessed remotely by connecting to the VPN. The IT Manager reviews backup logs on a weekly basis to identify any failures.

### ***Recommendation***

Prioritise finalising the Disaster Management Policy, and ensure it identifies critical information required for business continuity.

## **Storage**



Good storage is a very important factor for information protection and security. Appropriate storage arrangements for both physical and digital information ensures information remains accessible and usable for as long as it is required for business and legal purposes and for accountable government.

## **TOPIC 16 – Appropriate storage arrangements**

**Progressing**

### ***Summary of findings***

NPMT has some protection and security controls in place for physical and digital information. Physical information stored locally at NPMT's Auckland premises is primarily non-current financial records over 10 years old. Information is not appropriately labelled, and some boxes are stored on the floor. There is evidence of appropriate protection against identified hazards, such as fire and theft as the storage rooms have a sprinkler system and burglar alarm installed. Physical information is stored in locked storage rooms, and access is limited to approved personnel. However, no access log is maintained for storage rooms.

The majority of NPMT's digital information is stored on shared network drives, with additional information saved to relevant systems, such as the HR management system, and various Google drives linked to NPMT Gmail accounts. SAN host data and virtual machines are fully

backed-up using disc imaging. Backup data is kept outside the server room in the basement to protect against potential hazards in the server room, such as fire. Offsite digital storage options, such as the greater uptake of Cloud storage or physical removal, are being considered to enhance protection against ransomware attacks.

Backups are accessible over the network, and the retention period is typically between three to six months. Full back-ups are combined with incremental backups to minimise the risk of failure. The backup process covers various systems, including the radio playout system in Auckland and Wellington, as well as user profiles and desktops where many people store their files. NPMT also keeps permanent back-ups of financial information stored on the financial management system.

### ***Recommendation***

Identify risks to the information storage environments and plan to address these.

## **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**

## **Beginning**

### ***Summary of findings***

NPMT takes a decentralised approach to IM, where each business unit is responsible for managing information on the systems they use. As a result, the use of shared network drives is inconsistent across NPMT. There are no file plans or naming conventions in place. Staff acknowledged that these would improve information access and use across the organisation.

Access to information is controlled through restricted access to systems and files, including shared network drives. For example, access to HR information stored in these drives is appropriately restricted. Interviews confirmed that staff generally have adequate access to systems to find and use the necessary information. The IT Manager has a good understanding of the different levels of access controls. However, these controls have not been documented.

Three digital systems were reviewed as part of the audit. None of the systems reviewed complied with the minimum metadata requirements of Te Rua Mahara. Staff interviewed also noted that there is no consistent approach to using metadata for finding and managing information.

## ***Recommendations***

Develop consistent naming conventions for use in the shared drives.

Investigate options for replacing shared drives.



## **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 Te Rua Mahara (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***

There is no current and approved organisation-specific disposal authority covering information relating to all business functions and formats. NPMT has never had a disposal authority in place and there is no plan to develop one.

#### ***Recommendations***

Discuss the development of an organisation-specific disposal authority with Te Rua Mahara.

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

**Beginning**

#### ***Summary of findings***

NPMT is only authorised to dispose of information under the two General Disposal Authorities as it does not have a current and approved organisation-specific disposal authority.

No processes are in place to ensure information is retained for as long as required for business use. Staff confirmed that undocumented and ad-hoc disposals take place for physical and digital information. For example, the email accounts of staff who have recently left the organisation are usually deleted unless there are reasons to preserve the records they contain, such as their seniority. While the email accounts of recently departed staff are suspended, the IT Manager retains full access to email accounts for 6 months following the departure, which increases to 2 years for senior executive staff.



There was a digitisation project to upload financial records to the financial management system. There is no plan to dispose of the physical copies of the digitised financial records. Consequently, information is being duplicated across physical and digital formats. Additionally, information is duplicated across digital systems, such as governance documents which are stored in shared networks drives and a governance management system.

Staff use of uncontrolled environments increases the risk that digital information may have been disposed of in a manner inconsistent with the General Disposal Authorities.

***Recommendation***

Develop and agree a disposal policy for the organisation and plan to implement under the General Disposal Authorities.

**TOPIC 22 – Transfer to Te Rua Mahara**

**Not applicable**

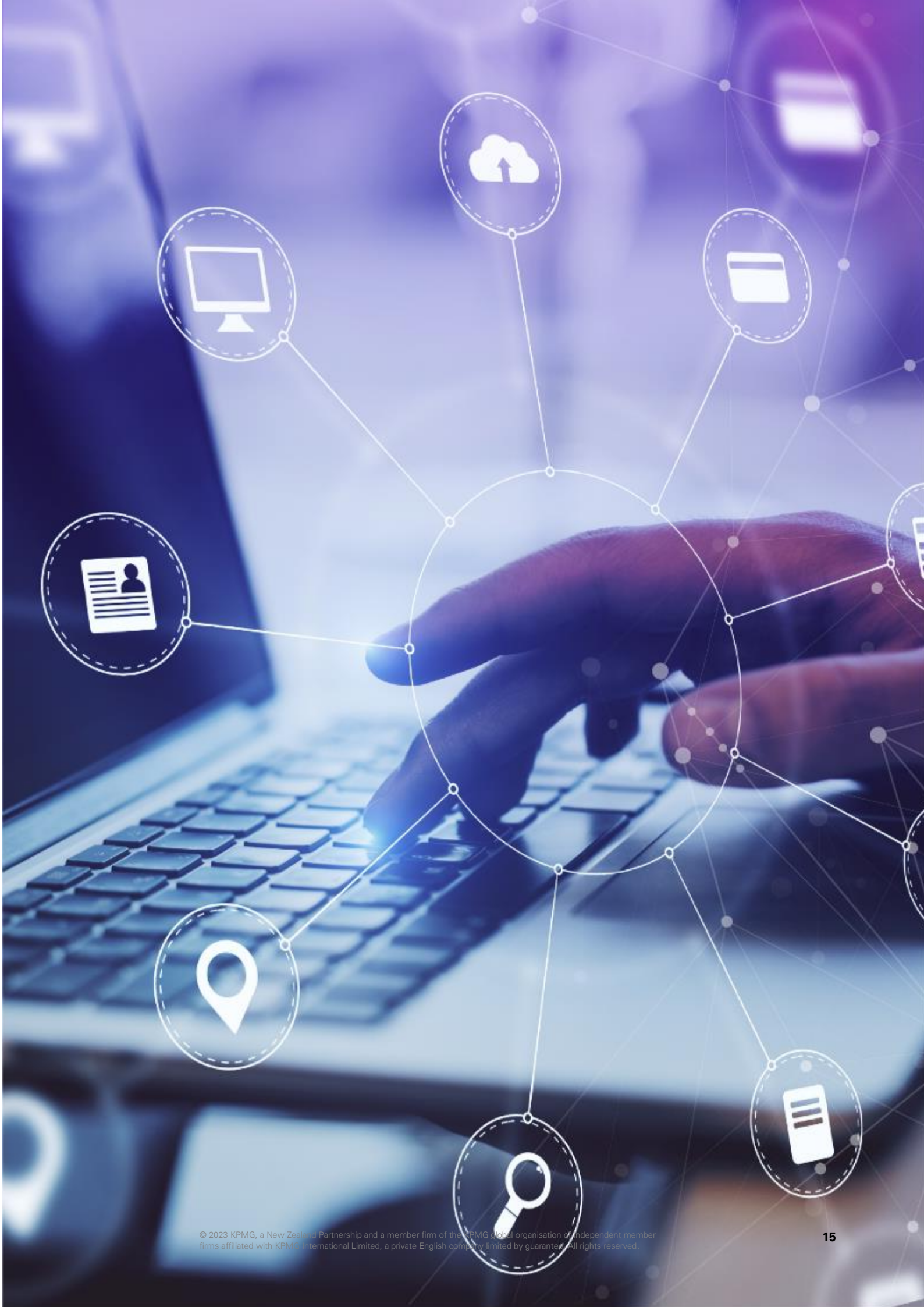
---

***Summary of findings***

As NPMT was established in 2002, it is not required to identify physical or digital information over 25 years of archival value.

***Recommendation***

Due to the not applicable assessment, we have not made a recommendation.



## 6. Summary of feedback

The National Pacific Media Trust (formerly The National Pacific Radio Trust) is committed to fulfilling our obligations under the Public Records Act 2005 and our Deed of Trust as it pertains to archiving broadcast content.

Our current funding contract with NZ On Air relates to operating two radio stations.

We are in the midst of transitioning to a digital multi-media broadcaster.

Our future funding relationship with NZ On Air will reflect this transformation of our operating model.

We have recently agreed a Memorandum of Understanding with Radio New Zealand which includes how we can support one another on achieving efficiencies within our respective operations.

## 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 – Beginning

Topic 2, IM policy and processes – Beginning

Topic 3, Governance arrangements and Executive Sponsor – Progressing

Topic 4, IM integration into business processes – Beginning

Topic 5, Outsourced functions and collaborative arrangements – Beginning

Topic 6, Te Tiriti o Waitangi – Progressing

Topic 7, Self-monitoring – Beginning

Topic 8, Capability and capacity - Beginning

Topic 9, IM roles and responsibilities - Beginning

Topic 10, Creation and capture of information - Beginning

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

Topic 12, IM requirements built into technology systems - Beginning

Topic 13, Integrity of information - Progressing

Topic 14, Information maintenance and accessibility - Beginning

Topic 15, Business continuity and recovery – Beginning

Topic 16, Appropriate storage arrangements – Progressing

Topic 18, Information access, use and sharing – Beginning

Topic 20, Current organisation-specific disposal authorities – Beginning

Topic 21, Implementation of disposal decisions – Beginning

Topic 22, Transfer to Te Rua Mahara – Not applicable

[kpmg.com/nz](https://kpmg.com/nz)



12 April 2024

Te Rua Mahara o te Kāwanatanga Archives New Zealand  
10 Mulgrave Street  
Wellington

Don Mann  
Chief Executive  
National Pacific Media Trust  
Don.Mann@pmn.co.nz

Phone +64 499 5595

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

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

E te rangatira e Don, Fakaalofa lahi atu, Ni sa bula, Mālo e lelei, Kia orana, tēnā koe

## Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the National Pacific Media Trust (NPMT) 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 (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*

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 NPMT is assessed as operating at very low IM maturity and is at the start of its improvement journey.

Your commitment to fulfilling obligations under the PRA is noted in the audit report summary of feedback alongside a new opportunity to work with Radio New Zealand for support. This support could help NPRT to establish an IM Policy, Strategy and adequate systems to provide a sturdy platform for improvement. We are also available to assist your IM improvement work in the audit follow up which runs for a two-year period.

It is disturbing to read of the reported loss of audio recordings for a year's worth of radio broadcasts in Topic 14: *Information maintenance and accessibility*. As this is potentially unauthorised disposal, we will be in touch outside of the audit follow up to learn more about what was disposed of and how we may be able to help you to ensure that it doesn't reoccur.

### **Prioritised recommendations**

The audit report lists 20 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.

Fakaaue lahi, Vinaka vakalevu, Mālo aupito, Ia manuia, Meitaki maata, Nāku iti noa, nā



Anahera Morehu  
Poumanaaki Chief Archivist  
**Te Rua Mahara o te Kāwanatanga Archives New Zealand**  
Cc The Chief Executive is the Executive Sponsor



## APPENDIX

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
<b>Governance</b>	1: IM strategy	<i>Develop an IM Strategy or integrate one within a related strategic document following guidance from Te Ru Mahara. The Strategy should be approved by senior management, communicated to all staff and contractors, and reviewed on a periodic basis to ensure it continues to support NPMT's business needs and the strategic direction of the organisation.</i>	Development of an IM Strategy and associated work plan is a useful starting point for IM improvement. Some specialist IM advice would be advisable to ensure the organisation is well supported. <a href="#">Information and records management strategy</a>
<b>Governance</b>	2: IM policy and processes	<i>Develop an IM Policy, and associated processes and guidance in consultation with staff. Communicate these throughout the organisation.</i>	Considering the size of the organisation and capacity of staff, this could also be scoped into initial work by an IM specialist to ensure that the necessary areas of IM operation are covered. Appropriate naming conventions could be covered here - recommendation for Topic 18: <i>Information access, use and sharing</i> . <a href="#">Information and records management policy development</a>
<b>Capacity</b>	8: Capacity and capability	<i>Assess NPMT's IM capacity and capability against business needs and plan to address these internally or with external assistance.</i>	Once the Strategy, work plan and Policy are agreed the organisation will know what resource is needed to support IM improvement.
<b>Creation</b>	10: Creation and capture of information	<i>Include in the IM Policy the requirement for staff to use the organisation's systems and monitor this.</i>	It is a basic requirement that the organisation creates and maintains full and accurate records that are accessible for as long as required. The systems used for storing records need to be fit for purpose and our mandatory standard identifies system requirements. <a href="#">Information and records management standard</a>

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Management	13: Integrity of information	<i>Develop and socialise a process for the shared drive that ensures consistent practice across the organisation.</i>	This would help productivity by supporting staff to find information more easily.
Management	14: Information maintenance and accessibility	<i>Assess risks to the ongoing accessibility of digital and physical information and plan to address the risks.</i>	This includes formats and systems. Also relevant to recommendations for Topic 16: <i>Appropriate storage environments</i> . Please note that backups are for disaster recovery situations rather than digital preservation.
Disposal	21: Implementation of disposal decisions	<i>Develop and agree a disposal policy for the organisation and plan to implement under the General Disposal Authorities.</i>	This will require specialist IM advice and will give the organisation assurance that information is being retained for as long as is required - an important first step with disposal. When agreed the disposal policy should be communicated to staff to ensure they are aware of the requirements. It is also important that the current disposal action is completed within the terms of the General Disposal Authorities, and that this disposal is fully documented in a disposal register.