Public Records Audit Report for Telarc Limited

Prepared for Te Rua Mahara o te Kāwanatanga Archives New Zealand

January 2024

kpmg.com/nz

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 Telarc Limited elements of any report we provide to you under the terms of this engagement. In this event, we will not require Telarc Limited 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 Telarc Limited. 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, Telarc Limited 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

1. Executive summary

Established in 1972, Telarc Limited (Telarc) is a Crown Entity Subsidiary fully owned by the International Accreditation Council of New Zealand (IANZ). Telarc is recognised by the Joint Accreditation System – Australia and New Zealand (JAS-ANZ) as a certification/registration body for quality, environmental, and safety management systems. Telarc focuses on both compliance and business improvements in its auditing services for clients across New Zealand.

Telarc creates and maintains public records across its operations, including fieldwork documentation from client audits, client audit reports, certification details and corporate records.

Telarc's digital information is primarily stored in an Enterprise Content Management system (ECM) and historical information is held in shared drives. Client information is managed through a Client Relationship Management (CRM) system. Physical records are stored at a third-party storage provider.

Certain services, including information management (IM), financial, company secretarial, training centre, administrative, and Information Technology (IT) services, are outsourced to Telarc's parent organisation, IANZ, through a Master Services Agreement (MSA).

Telarc employs 45 full-time equivalent staff. The Executive Sponsor is the CEO and IM is handled collectively by various individuals across Telarc and IANZ, including the Operations Support Manager, Technical Managers, Certification Managers, scheduling staff, and Programme Manager - GLP Compliance Monitoring. Although there is no dedicated Information Manager, IM and IT expertise is provided by IANZ under the MSA.

Telarc's IM maturity is summarised below. Further detail on each of the maturity assessments can be found in sections 4 and 5 of this report.

Beginning	**8**
Progressing	**10**
Managing	**2**
Maturing	**0**
Optimising	**0**

2. Introduction

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

Telarc's 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 Telarc including both physical and digital information.

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

The audit reviewed Telarc 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 Telarc's key systems that act as a repository for public records. The systems assessed were Telarc's ECM, CRM, and audit reporting tool. 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. Telarc 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 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	●				
Self-monitoring							
	7	Self-monitoring	●				
Capability							
	8	Capacity and capability		●			
	9	IM roles and responsibilities		●			
Creation							
	10	Creation and capture of information		●			
	11	High-value / high-risk information	●				
Management							
	12	IM requirements built into technology systems		●			
	13	Integrity of information		●			
	14	Information maintenance and accessibility			●		
	15	Business continuity and recovery	●				
Storage							
	16	Appropriate storage arrangements		●			
Access							
	18	Information access, use and sharing		●			
Disposal							
	20	Current organisation-specific disposal authorities	●				
	21	Implementation of disposal decisions	●				
	22	Transfer to Te Rua Mahara	●				

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

Telarc does not have a dedicated IM Strategy to provide strategic direction and support for IM within the organisation. There is appetite from the Executive Sponsor and IM staff to implement an IM Strategy. However, there are no clear timeframes for developing and implementing the Strategy.

Although there is no strategy for IM, senior management support Telarc's IM practices through the Technology Upgrade Programme. The Executive Sponsor intends to use information held by Telarc to gain insights into industry changes and improvements for clients under a new operating model. Recent investments in technology support this initiative, including the development of an audit reporting tool and CRM upgrades.

The initial phase of the Technology Upgrade Programme is documented in the 'Business Case Request for Capital Approval' from December 2021. Some elements of the document could be incorporated into an IM Strategy, such as key IT initiatives focused on enhancing Telarc's data management.

Recommendation

Develop an IM Strategy using the guidance from Te Rua Mahara. The Strategy should support the business needs and strategic direction of the organisation.

TOPIC 2 – IM policy and processes — Progressing

Summary of findings

There is no overarching IM Policy in place. However, process documents that contain IM roles and responsibilities exist in the process management system. For example, staff who generate an audit report from a template in the ECM are responsible for manually completing certain metadata, such as document and assessment type. Staff interviewed were aware of and understood their roles and responsibilities for IM.

There are high-level plans from the Executive Sponsor and IM staff to develop and implement an IM Policy. There are no clear timeframes for developing and implementing the Policy. Such a Policy will likely be developed in conjunction with Telarc's outsourced services provider under the MSA.

Recommendation

Develop an overarching IM Policy to provide formal guidance to staff. The Policy should be linked to the Strategy, contain roles and responsibilities and align with the requirements of Te Rua Mahara and relevant legislation.

TOPIC 3 – Governance arrangements and Executive Sponsor — Progressing

Summary of findings

Due to the small size of the organisation, there is no dedicated IM governance group in place. Staff interviewed indicated responsibility for IM would likely sit with the Senior Leadership Team (SLT), which includes the Executive Sponsor and Operations Support Manager. However, IM is not regularly, formally addressed as part of SLT meetings. Instead, IM issues are addressed on an ad hoc basis.

The Executive Sponsor is aware of their oversight and monitoring role and has fulfilled this by ensuring IM was considered within the implementation of the process management system and audit reporting tool. However, there is no regular or formal reporting on IM activities to the Executive Sponsor.

Recommendation

Decide which governance group will cover IM and include in the ToR or as a regular agenda item.

TOPIC 4 – IM integration into business processes — Managing

Summary of findings

Responsibility for the management of information within business units is consistently assigned to business owners, with team members having a strong awareness of their responsibility to integrate IM into business processes and activities. However, staff do not receive regular IM specific training.

IM is integrated into most business processes and activities due to the nature of Telarc's role as an auditor. The process management system documents IM requirements, such as saving all audit reports to the ECM, and includes links to document templates to ensure staff capture all the required information.

IM expertise is regularly included in business process change and development. For example, IM expertise was provided during the implementation of the ECM under the MSA in 2015. The Executive Sponsor also plays a key role in the Technology Upgrade Programme.

Issues with the management of information that impact business processes and activities are directed to appropriate staff for action. Process owners assigned in the process management system are responsible for addressing corrective actions identified. For example, Technical Managers are responsible for updating audit processes to align with current best practice, which includes updating any relevant IM requirements. Additionally, process owners conduct annual audits over process documentation. Updates to process documentation are highlighted in the system to effectively communicate changes to staff.

Recommendation

Following completion of the IM Policy and Strategy, assess the need for IM training and develop a fit-for-purpose programme.

TOPIC 5 – Outsourced functions and collaborative arrangements — Progressing

Summary of findings

IM roles, responsibilities and requirements were identified in some, but not all, contracts sampled for outsourced functions and collaborative arrangements. For example, the contractor agreement template used to engage auditor sub-contractors specifies that all audits must be recorded in full and returned to Telarc in electronic format. It also states that Telarc retains ownership of all corporate information provided to sub-contractors. However, the MSA does not mention any IM requirements beyond those relating to handling confidential information.

Only one contract reviewed recognised the status of documents handled as public records.

Telarc monitors audit sub-contractors against their IM obligations, to the extent they are directly related to audit deliverables, such as audit reports required for certification. This monitoring activity does not cover all contracts where there are outsourced functions or collaborative arrangements.

Recommendation

Ensure all contracts for outsourced functions or collaborative arrangements include roles and responsibilities for IM, and that monitoring is done to check that requirements are met, including for the sub-contractors.

TOPIC 6 – Te Tiriti o Waitangi — Beginning

Summary of findings

Telarc has not identified any information of importance to Māori. There is limited capability within Telarc to incorporate and maintain metadata in te reo Māori. As a result, Telarc has not been able to improve the accessibility and discovery of information of importance to Māori.

Recommendation

Identify whether Telarc holds information that is of importance to Māori. The outcome of this exercise will inform Telarc what further actions are required to address this topic.

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 — Beginning

Summary of findings

There is currently no monitoring of compliance with IM requirements detailed in the PRA, the Standard, and other relevant legislation due to the absence of an IM Policy. There are no monitoring activities or proposed corrective actions being reported to the Executive Sponsor or the senior leadership team.

However, internal IM processes are regularly monitored in relation to client audits and certification processes. Proactive peer reviews are conducted over all client audits, and corrective actions are addressed before finalising audit reports to ensure they are complete and accurate records. Certification decisions are reviewed using a checklist to verify that processes, including relevant IM processes, were followed by staff.

While Telarc has identified key compliance obligations under the PRA, such as only disposing of records with the authority of the Chief Archivist, no measures have been taken to ensure compliance. As a result, corrective actions to address compliance are inconsistently managed across the organisation.

Recommendation

Once the IM Policy has been developed, design and implement regular IM monitoring procedures, and report useful and actionable information to the Executive Sponsor.

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 — Progressing

Summary of findings

The Executive Sponsor and Operations Support Manager have appropriate IM capability to support some business needs. IM expertise has been engaged in the past under the MSA, where further IM capability has been required. However, staff acknowledge the need for improvement in their understanding of the PRA.

Given the size of the organisation, and the number of responsibilities the Executive Sponsor and Operations Support Manager have which are not related to IM, there is limited capacity to uplift Telarc's IM. Hiring additional IM staff is not seen as viable given the limited resources available within the organisation. Instead, the Executive Sponsor suggested that the MSA could be leveraged to address Telarc's current IM capacity needs, although this would need to be negotiated with IANZ.

Recommendation

Assess what IM resources are required to support Telarc's needs, and if they are available internally or need to be contracted externally.

TOPIC 9 – IM roles and responsibilities — Progressing

Summary of findings

Telarc staff have some awareness of their IM responsibilities. Staff complete induction training as part of onboarding. This training includes instruction on using the ECM and CRM, and provides an overview of various business processes, including relevant IM requirements.

Staff have not been provided with targeted, ongoing IM training. No plan has been made to develop this. Once the IM Strategy is in place, Telarc has expressed intent to support self-guided IM training for all staff.

Roles and responsibilities for IM are not documented in all job descriptions and performance plans for staff and contractors. The three job descriptions sampled as part of the audit contained only limited reference to PRA requirements, such as maintaining accurate records. Staff noted that performance plans for Auditors contain more detailed requirements regarding compliance with IM requirements.

While Telarc's Code of Conduct does not refer to any IM roles and responsibilities, it requires staff to comply with all Telarc policies and processes. As IM requirements are captured in Telarc's business processes, staff must comply with these requirements.

Recommendation

Ensure IM roles and responsibilities are detailed in the IM Policy and communicated to all staff and contractors.

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 understand and comply with their obligations to create full and accurate records. They actively ensure that the right information is routinely created and captured as part of all business functions and activities. Minimum metadata requirements are met in the ECM. Staff are confident in the reliability and trustworthiness of the information they find in the ECM due to the metadata processes that are in place.

Scheduling staff regularly update client information in the CRM to ensure it is complete and accurate. There is a structured approach to monitoring and addressing information usability and reliability issues in the process management system, which includes a module used to identify and address corrective actions as required. Business process owners are consistently assigned across the organisation, and staff conduct annual reviews over the information in the process management system.

However, sub-contractor auditors do not have access to Telarc's IM systems, such as the ECM and CRM. Therefore, they use uncontrolled environments, such as personal devices and external drives to create and capture information. Information transfers between Telarc and sub-contractor auditors typically occur via email. Staff confirmed that a new file sharing system will be implemented to grant the sub-contractor auditors' access to the necessary information.

Recommendation

Continue work to implement the new file sharing system to ensure all information is created and captured on controlled systems.

TOPIC 11 – High-value / high-risk information — Beginning

Summary of findings

Telarc has not formally identified information assets as high-value or high-risk. As a result, there is no consistent understanding of what information is considered high-value or high-risk across the organisation.

Telarc does not have a documented inventory of the information it holds in both digital and physical storage, making it difficult to establish a long-term management plan for this type of information.

Recommendation

Create an information asset register that identifies the information that is high-value or high-risk to Telarc.

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 — Progressing

Summary of findings

Due to the size of the organisation, the Executive Sponsor is involved with design and configuration decisions relating to new and upgraded business systems, alongside the Operations Support Manager. IT expertise is provided by IANZ, under the MSA, and IM requirements are considered in the design, configuration, documentation and implementation of new business systems and decommissioning of old business systems. For example, the Executive Sponsor played a key role in the Technology Upgrade Programme, and ensured minimum metadata requirements were incorporated to improve document retrieval in the ECM. However, system design and configuration is not fully documented or maintained for all business systems.

There are no standardised IM requirements for new and upgraded business systems documented.

Recommendation

Identify and document standardised IM requirements for new and upgraded business systems.

TOPIC 13 – Integrity of information — Progressing

Summary

Organisation-wide IM practices are in place and routinely followed to ensure that information is reliable and trustworthy. Staff interviewed noted that information is easy to find, reliable and trustworthy, including historical information stored on shared drives as this information remains accessible on the ECM. However, staff also noted that sub-contractors have variable experiences when trying to find and retrieve information as they cannot access the ECM.

There is strong messaging from the SLT emphasising the importance of maintaining the integrity of information, which was reflected in business process documentation and through interviews.

A variety of management controls and IM requirements are integrated into business processes and IM systems to promote the integrity of information across the organisation. Access controls are in place to limit file access and editing to relevant staff. For example, only the appropriate staff can approve a leave request in the ECM. Audit logs are automatically stored in the ECM to help staff maintain the integrity of information by tracking actions, such as creation, access, and modification. The version history function in the ECM allows staff to restore a file to a previous version and manage changes made to a file over time.

The CRM contains relevant data fields required to ensure appropriate information about Telarc's clients is captured. Specific data fields from the CRM automatically populate some metadata in the ECM, such as the file type and client short name. Audit reports created in the ECM from the CRM are named according to system-enforced file naming conventions.

Recommendation

Refer to the recommendation for Topic 10 – *Creation and Capture of Information*.

TOPIC 14 – Information maintenance and accessibility — Managing

Summary of findings

There are strategies in place to manage and maintain physical and digital information during business and system changes. For example, during the restructuring of the CRM, testing procedures were conducted to ensure the accurate transfer of client data between the old and new structure. Historical digital files remain accessible through the ECM, although these are stored on shared drives and not in the ECM.

All physical records are held in a third-party commercial storage facility. A register of physical information is maintained by the third-party and is available on request. The register provides access to the records and use of a third-party commercial storage facility reduces the risk of physical damage.

Telarc is aware of risks to the ongoing accessibility of physical information and technology obsolescence, such as outdated business systems. While these risks are not identified in the organisation's risk register and there are no documented plans to mitigate them, some measures are in place to mitigate technology obsolescence risks. For example, Telarc maintains M-files as an 'evergreen' product by performing regular system updates.

Recommendation

Identify and document all risks relating to technology obsolescence in Telarc's risk register and plan to eliminate or mitigate these risks as much as possible.

TOPIC 15 – Business continuity and recovery — Beginning

Summary of findings

Telarc's Crisis Preparedness and Reputation Management (CPRM) plan was last updated in June 2022. The document does not identify critical information that would require restoration.

The restoration of digital information is managed by Telarc's outsourced IT provider under the MSA. Restoration plans are tested quarterly, and staff can access digital information remotely.

The CPRM plan does not reference physical information. However, physical information is stored at a commercial storage provider and is not required for regular business activities.

Recommendation

Update the CPRM plan to include critical information required to ensure 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

Telarc has protection and security controls in place for physical and digital information.

Telarc uses third-party storage providers for digital and physical information, which provide protection against unauthorised access, loss, deletion, or destruction. There are adequate password protections and access controls in place. For example, digital information is tagged by staff with the document classification. Once tagged, the ECM automatically updates document permissions based on the type of information. Staff must connect to a virtual private network (VPN) to access systems remotely, which requires dual authentication.

Telarc does not regularly test its protection and security processes, although some aspects of cybersecurity are monitored by Telarc's outsourced IT provider under the MSA.

Recommendation

Implement testing of protection and security processes.

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 — Progressing

Summary of findings

Telarc consistently uses metadata to facilitate the management and discovery of digital information. The minimum metadata requirements issued by Te Rua Mahara are embedded into the ECM. Additional metadata fields are included in virtual folders in the ECM, such as client short name, to increase accessibility of information. Some historic digital information remains on shared drives, which does not meet minimum metadata requirements.

Staff and contractors know how to use the ECM to access information, as this is included in induction training. For example, staff can personalise their view settings within the ECM based on metadata tags to support quick access to information. When an issue with finding information is encountered, the Operations Support Manager and scheduling staff provide support and advice.

Staff have a good understanding of how the business manages access to certain files. Telarc's outsourced IT provider has administrative rights to update permissions if required. The ECM also offers visibility over who has access, read, and edit rights for individual documents. These access controls for physical and digital information are not formally documented.

Telarc typically uses email to share information externally. However, as referenced in Topic 10 – *Creation and Capture of Information*, Telarc is currently implementing a file-sharing system linked to its ECM that will enable secure sharing of information with external parties as part of its IT transformation.

Recommendation

Document access controls for physical and digital information and implement regular reviews to ensure the controls remain appropriate.

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 (DA). Telarc has never had a DA since its establishment in 1973. The embedded practice at Telarc is to retain all information.

Recommendation

Develop an organisation-specific disposal authority and obtain approval from Te Rua Mahara.

TOPIC 21 – Implementation of disposal decisions — Beginning

Summary of findings

Telarc is only authorised to dispose of information under the two General Disposal Authorities (GDAs) as it does not have a current and approved organisation-specific DA.

Staff noted that Telarc retains all information indefinitely and that no disposals have taken place. No information has been completely deleted from IM systems, including the ECM and CRM. If information is accidentally deleted, it can be recovered by Telarc's outsourced IT provider under the MSA.

There is no plan to monitor and manage information to enable regular disposal decisions to be made. This poses the risk that Telarc will be holding onto information for longer than necessary. Use of uncontrolled environments, such as contractors' personal drives, increases the risk that digital information has been disposed of in a manner inconsistent with the GDAs.

Recommendations

Develop a disposal implementation plan and assess the resources necessary to perform disposal actions.

Include contractors' personal drives in the disposal implementation plan.

TOPIC 22 – Transfer to Te Rua Mahara

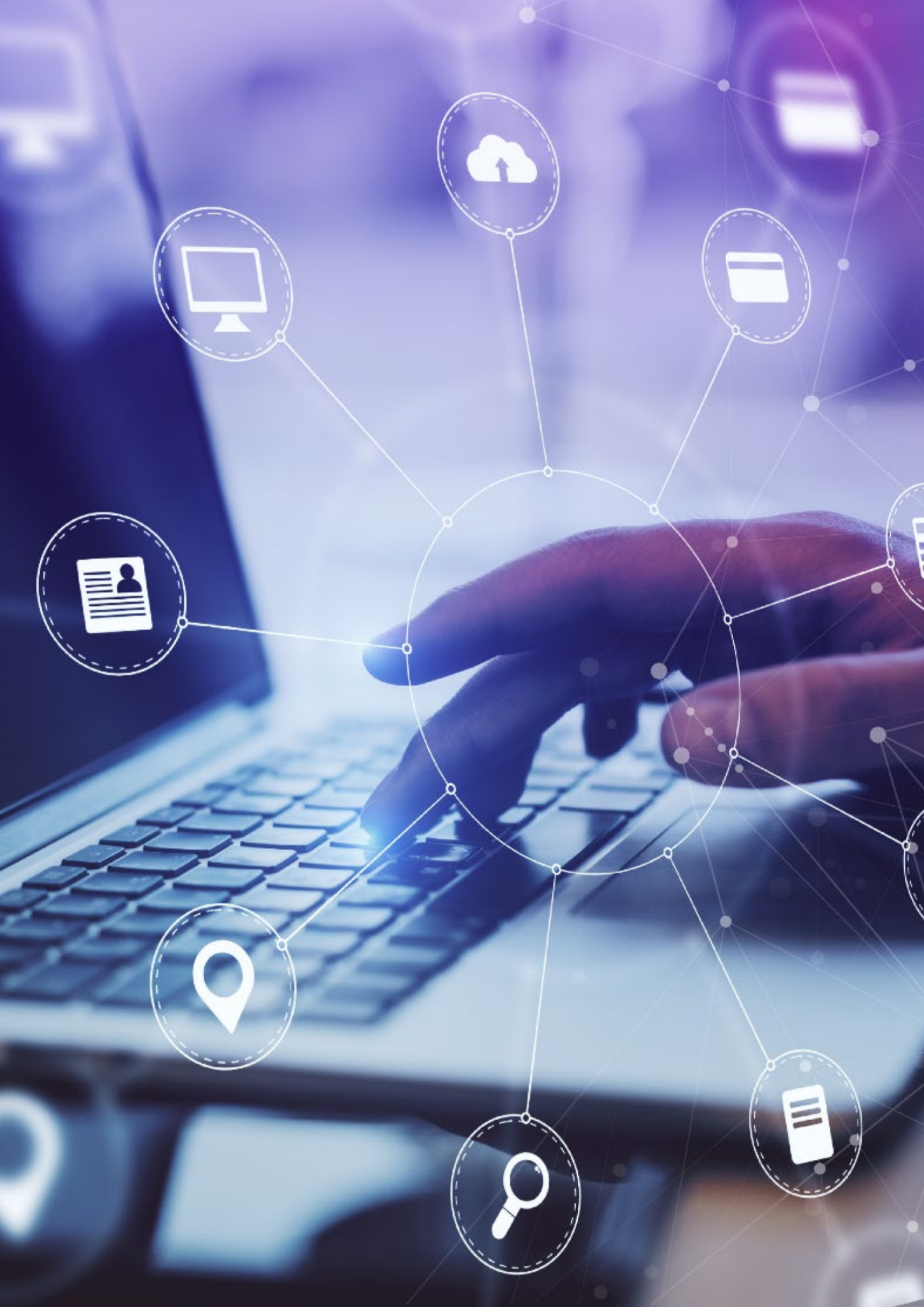
Beginning

Summary of findings

Physical and digital information of archival value over 25 years old has not been identified. Telarc has never transferred information in physical or digital format to Te Rua Mahara and there is no plan to make a transfer.

Recommendation

Identify physical and digital information of archival value under GDA 6 that is over 25 years old.



6. Summary of feedback

Telarc did not provide any feedback for this section.

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 – Progressing

Topic 3, Governance arrangements and Executive Sponsor – Progressing

Topic 4, IM integration into business processes – Managing

Topic 5, Outsourced functions and collaborative arrangements – Progressing

Topic 6, Te Tiriti o Waitangi – Beginning

Topic 7, Self-monitoring – Beginning

Topic 8, Capability and capacity – Progressing

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 – Progressing

Topic 13, Integrity of information – Progressing

Topic 14, Information maintenance and accessibility – Managing

Topic 15, Business continuity and recovery – Beginning

Topic 16, Appropriate storage arrangements – Progressing

Topic 18, Information access, use and sharing – Progressing

Topic 20, Current organisation-specific disposal authorities – Beginning

Topic 21, Implementation of disposal decisions – Beginning

Topic 22, Transfer to Te Rua Mahara – Beginning

kpmg.com/nz

21 August 2024

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

Philip Cryer
Chief Executive Officer
Telarc Limited
Philip.cryer@telarc.co.nz

E te rangatira e Philip, tēnā koe

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of Telarc Limited 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.

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. Telarc's IM is assessed as operating at the lower end of the maturity scale.

However, information relating to Telarc's core business with audit clients and certification processes is well-managed, for example sub-contractors are audited against their IM obligations. This good work should be mirrored for the corporate side of the business which is less well-managed. Another example is where performance plans for auditors include more detailed requirements for IM compliance than for other work roles.

All three topics in the disposal category are assessed at the 'Beginning' maturity level. This should be identified as a risk on the organisation's risk register. Over-retention of information exposes the organisation to unnecessary storage costs, potential privacy issues and excessive work related to official information requests as well as requiring staff to manage and search through more information than is needed.

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 nine recommendations as identified in the Appendix.

What will happen next

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

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

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

Thank you again for your support with the audit. We would greatly appreciate further feedback on the audit process and the value it provides to organisations. We have sent a feedback survey link for the attention of your Executive Sponsor in the accompanying email.

Nāku iti noa, nā

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

Cc The Chief Executive is the Executive Sponsor

APPENDIX

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Governance	1: IM strategy	*Develop an IM Strategy using the guidance from Te Rua Mahara. The Strategy should support the business needs and strategic direction of the organisation.*	The strategy doesn't need to be a stand-alone document but could be incorporated into other governance strategies. Information and records management strategy
Governance	2: IM policy	*Develop an overarching IM Policy to provide formal guidance to staff. The Policy should be linked to the Strategy, contain roles and responsibilities, and align with the requirements of Te Rua Mahara and relevant legislation.*	When this is well communicated to staff, it will promote common awareness of IM roles and requirements. Information and records management policy development
Governance	3: Governance arrangements and Executive Sponsor	*Decide which governance group will cover IM and include in the TOR or as a regular agenda item.*	A governance group that includes IM would provide support for the Executive Sponsor. Through regular IM reporting, the group would support the organisation to improve IM maturity through awareness of IM trends and issues and support work to address these as appropriate.
Self-monitoring	7: Self-monitoring	*Once the IM Policy has been developed, design and implement regular IM monitoring procedures, and report useful and actionable information to the Executive Sponsor.*	Internal IM processes are used to regularly monitor the audit clients and certification processes including peer reviews and corrective actions. However, there is no monitoring for the corporate side of the business which has affected the rating assessment.
Capacity	8: Capacity and capability	Assess what resources are available to support Telarc's needs and if they are available internally or need to be contracted externally.	Even though a small organistion, Telarc still needs access to IM expertise to set up IM strategy, policy and processes relevant to its size and importance of information.

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Creation	10: Creation and capture of information	*Continue work to implement the new file-sharing system to ensure all information is created and captured on controlled systems.*	This would be a useful upgrade to ensure that sub-contractors can access Telarc's systems for creation of information and management across its life-cycle mitigating access issues.
Creation	11: High-value/High-risk information	*Create an information asset register that identifies the information that is high-value/high-risk to Telarc.*	Developing an information asset register can also assist with the work needed to address Topic 15: Business continuity and recovery. Information assets overview
Management	15: Business continuity and recovery	*Update the CPRM to include critical information required to ensure business continuity.*	This would be useful to ensure that the organisation understands where its critical information is and its value.
Disposal	21: Implementation of disposal decisions	*Develop a disposal implementation plan and assess the resources necessary to perform disposal actions.*	The risks of over retention of information should be assessed including cost and a plan developed for how disposal will be managed including potential development of an organisation specific disposal authority.