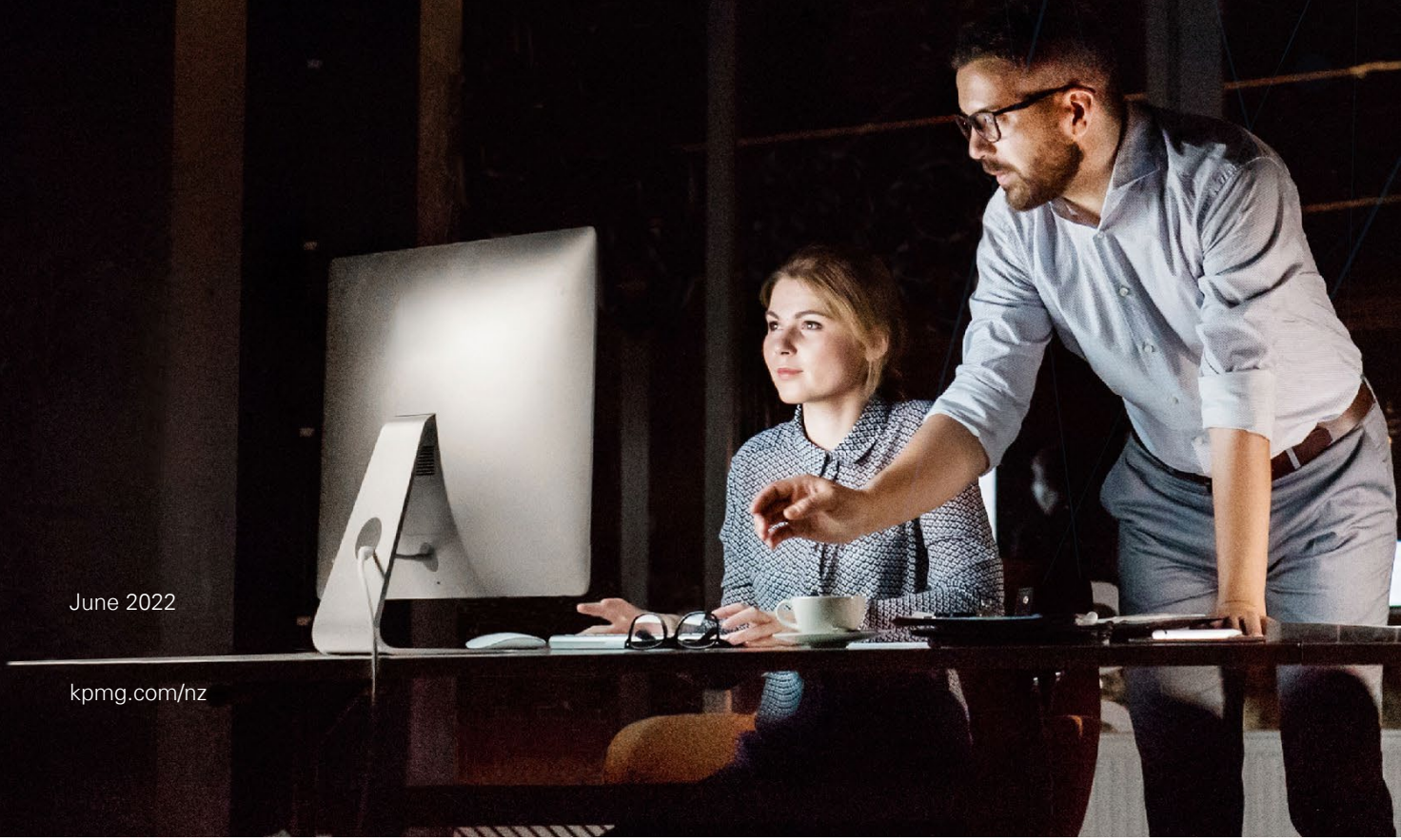
KPMG

Public Records Act 2005 Audit Report for the Electricity Authority

Prepared for Archives New Zealand



June 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 Electricity Authority. 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 Electricity Authority management and personnel consulted as part of the process.

Third Party Reliance

This report is solely for the purpose set out in the "Introduction" and "This Audit" sections of this report and for Archives New Zealand and the Electricity Authority 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

The Electricity Authority (the Authority) is an independent Crown entity responsible for overseeing and regulating the New Zealand electricity market. The Authority (previously named the Electricity Commission) was established in 2003 and became an independent Crown entity (thereafter named the Electricity Authority) in 2010.

The Authority creates high value public records relating to and including:

- electricity development records
- records of reviews and enquiries into the electricity market
- registration data
- recommendations to the Minister

The Authority has an Enterprise Document and Records Management System (EDRMS) as its primary method of managing information. The Authority maintains both physical and digital information. A third party storage provider holds all the Authority s physical records.

The Authority employs approximately 100 staff. In October 2021, the Authority underwent a restructuring of its information management function. There is one dedicated information management staff member (the Information Manager). However, at the time of the audit, this role was vacant.

The Authority does not have a dedicated governance group to oversee information management. In place of this, the Senior Leadership Team carries out this function.

The Authority 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	**13**
Managing	**0**
Maturing	**0**
Optimising	**0**
Not Applicable	**1**

2. Introduction

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

The Authority's information management 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 Authority including both physical and digital information.

The audit involved reviews of selected documentation, interviews with selected staff, including the Manager Data and Information Management (CISO), Chief Operating Officer, Procurement and Corporate Contract Management Lead, and a sample of other staff members from various areas of the Authority. *

The audit reviewed the Authority's information management practices against the PRA and the requirements in the Information and records management standard and provides an assessment of current state maturity. 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 Authority has reviewed the draft report, and a summary of their comments can be found in section 6.

**Note that the Executive Sponsor is the senior responsible officer for the audit. The Executive Sponsor was unavailable to speak with us at the time of the audit.*

4. Maturity Assessment

This section lists all assessed maturity levels by topic area. For further context about how each maturity level assessment has been made, refer to the relevant topic area in the report in Section 5.

Category	No.	Topic	Maturity				
			Beginning	Progressing	Managing	Maturing	Optimising
Governance							
	1	IM strategy	●				
	2	IM policy and processes		●			
	3	Governance arrangements & Executive Sponsor	●				
	4	IM integration into business processes		●			
	5	Outsourced functions and collaborative arrangements		●			
	6	Te Tiriti o Waitangi	●				
Self-monitoring							
	7	Self-monitoring	●				
Capability							
	8	Capacity and capability		●			
	9	IM roles and responsibilities		●			
Creation							
	10	Creation and capture of information		●			
	11	High-value / high-risk information	●				
Management							
	12	IM requirements built into technology systems		●			
	13	Integrity of information		●			
	14	Information maintenance and accessibility		●			
	15	Business continuity and recovery		●			
Storage							
	16	Appropriate storage arrangements		●			
Access							
	18	Information access, use and sharing		●			
Disposal							
	20	Current organisation-specific disposal authorities		●			
	21	Implementation of disposal decisions	●				
	22	Transfer to Archives New Zealand	Not applicable				

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

The Authority does not have an up-to-date information management strategy to provide strategic direction for information management activities. The Authority's last information management strategy was created in 2007, which was previously the Electricity Commissions strategy. The actions contained in this strategy had a time frame of three years and does not incorporate the recent business changes, such as the restructuring of the information management function.

The CISO indicated an intention to update the strategy to meet the organisation's current and future needs. However, the update had not yet started at the time of the audit.

Recommendations

Update the information management strategy following Archives New Zealand's guidance. The strategy should support business needs and strategic direction of the organisation.

TOPIC 2 – IM policy and processes

Progressing

Summary of findings

The Authority has a current Information and Data Management Policy. It was last reviewed and approved in June 2019 by the Board, Chief Executive and Chief Operating Officer.

The staff members interviewed were aware of an Information Data Management Policy and knew how to access the policy through the intranet if needed. Staff also had an awareness of how information needs to be created and maintained as this is communicated to them during the new starter induction training. In addition, emails are sent to staff if there are any changes or updates to organisation policies.

There are organisation-wide process documents available on the Authority's intranet. These include Information Security Procedures and Guidelines and a comprehensive EDRMS training guide.

The Authority is creating a new Information Management Policy by consolidating three legacy policies, including the ICT Acceptable Use Policy, the Information Security Policy and the Information and Data Management Policy. This consolidated policy is in draft form, and the CISO confirmed that it would be finalised over the coming months. The new draft policy refers to relevant legislation, including the Public Records Act and the Official Information Act. It does not refer to the Archives New Zealand mandatory standard or align with the current (out-of-date) Information Management Strategy (see Topic 1 – IM Strategy).

Recommendations

Complete work on the draft Information Management Policy for approval by the Senior Leadership Team.

TOPIC 3 – Governance arrangements and Executive Sponsor

Beginning

Summary of findings

The Authority does not have a dedicated information management governance group. Instead, the Senior Leadership Team undertake this function. However, there is no standing agenda item where information management is addressed.

Staff indicated that there is irregular reporting to the Executive Sponsor, such as when an issue needs to be escalated. Regular reporting and formalising information management in the Senior Leadership Team meetings, will support the Executive Sponsor to better champion information management across the Authority.

Recommendations

Plan and document information management reporting requirements that provides useful and actionable information for the Executive Sponsor and the wider Senior Leadership Team.

TOPIC 4 – IM integration into business processes

Progressing

Summary of findings

Staff interviewed were aware of their responsibilities for managing information within their business area. Information management responsibilities are outlined in the current Information and Data Management Policy. Information management responsibilities are also outlined in job descriptions.

Requirements for managing information are integrated into some business processes and activities through organisation-wide guidance documents. These include the Information Security Procedures & Guidelines and the comprehensive EDRMS training guide.

Recommendations

Ensure guidance documents detail the requirements for integrating the management of information into core business processes and activities.

TOPIC 5 – Outsourced functions and collaborative arrangements

Progressing

Summary of findings

Requirements for managing information are outlined in all sampled contracts for outsourced functions. These contracts specify the contracted party's information management obligations, including the creation, management, retention, portability, and security of information. However, there is no evidence that the Authority monitors the information management obligations detailed in these contracts for compliance.

Information management staff are not generally involved in writing or approving information management sections of outsourced functions or collaborative agreements.

Recommendations

Develop a process to monitor the compliance the information management requirements where public records are kept and managed.

TOPIC 6 – Te Tiriti o Waitangi

Beginning

Summary of findings

The Authority has not identified any information that is of importance to Māori. In addition, there is currently limited capability within the Authority to incorporate and maintain metadata in Te Reo Māori. As a result, the Authority has not been able to actively improve the accessibility and discoverability of information of importance to Māori.

Recommendations

Identify and assess whether the information held by the Authority is of importance to Māori. The assessment will inform the Authority whether 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

The information management requirements from the PRA, Official Information Act, and other relevant legislation are identified and documented within the current Information and Data Management Policy and the updated (draft) Information and Management Policy. However, there is no monitoring of compliance with these internal policies. The staff members interviewed mentioned that some managers monitor the storing and sharing of information, but this is undocumented and informally done.

Recommendations

Design and implement regular information management monitoring processes and report findings that provide 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 Authority has recruited a new information manager who will fill the current resourcing gap in information management capability and capacity. Currently, information management responsibilities are completed by various roles, such as Manager Data and Information Management, Procurement and Contract Management Specialist and external software expertise.

There is a plan to further address capacity needs by hiring a coordinator who will support the information manager with administrative tasks such as answering EDRMS system related queries.

Professional development opportunities are accessible to the information management staff where needed and when requested.

Recommendations

Ensure that IM capacity and capability requirements are regularly assessed and monitored against business needs.

TOPIC 9 – IM roles and responsibilities

Progressing

Summary of findings

The staff members interviewed were aware of their information management responsibilities, including the specific requirements related to their role. These responsibilities were covered in depth in all three job descriptions sampled. Staff and contractors undergo one-on-one information management induction training with the information manager (or external support while the role is vacant). In addition, staff provide on the job training to new starters through a buddy system, and further guidance is provided through an information management support inbox.

Informal reminders are sent to staff via email as required if any issues arise. Refresher training is provided on a one-on-one basis as requested, but staff expressed the need for regular training and refresher sessions.

Recommendations

Assess the business need for regular ongoing information management training to staff and contractors. For example, refresher training that staff are required to complete on an annual basis.

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 and contractors are aware of their legal obligations to create and capture full and accurate records through new starter induction training, on the job training and communication from the Authority.

The Authority's EDRMS automatically creates metadata that supports the usability, reliability, and trustworthiness of information. This reduces the need for users to enter or create metadata manually, thus supports consistency. The Authority meets Archives New Zealand's minimum metadata requirements for information stored on the EDRMS.

Staff indicated that they would generally save information in the EDRMS, ensuring usability and reliability of information through robust version control, search functionality and audit trails. However, there is no structured approach to monitoring and addressing information usability, reliability, and trust issues within systems used at the Authority.

Information is occasionally saved in uncontrolled environments such as shared network drives on corporate computers. Staff noted that managers would informally monitor their compliance with creating information in controlled environments.

Recommendations

Ensure all information on Shared Drives is created and captured on appropriate systems that meet Archives New Zealand minimum metadata requirements.

TOPIC 11 – High-value / high-risk information

Beginning

Summary of findings

The Authority has not formally identified any high-value or high-risk information assets it holds. However, there is some understanding of what information may be considered high-risk or high-value information, including information about how the electricity industry and market operates and valuable data and research information for future strategic information. This information is held in restricted EDRMS folders.

Without an inventory of this information, it is not possible to have a long-term management plan for this type of information. In addition, there is a risk that this knowledge could be lost by the organisation when staff depart from the Authority if it is not documented.

Recommendations

Identify high-value/high risk information assets based on the organisation-specific disposal authority.

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

Information management requirements are sometimes considered in the design and configuration decisions related to new and upgraded business systems. For example, when the Authority upgraded to the latest version of the EDRMS, the previous information manager was involved with the aspects of migration. However, no standardised information management requirements have been identified and documented for new and upgraded systems.

The Authority's ERDMS system captures all the minimum metadata requirements set out by Archives New Zealand.

Recommendations

Create standardised information management requirements for new and upgraded business systems.

TOPIC 13 – Integrity of information

Progressing

Summary of findings

The Authority has organisation-wide information practices which are routinely followed by staff. These include Information Security Procedures and Guidelines and a comprehensive EDRMS training guide. The information practices are in place to ensure information is reliable and trustworthy.

Management controls are in place to maintain the accessibility and integrity of the information in the EDRMS, including version control, roles-based permissions, and audit trails. However, the controls are not regularly tested.

The Authority has an advanced search function that allows staff to find and retrieve information that they create and manage. The staff members interviewed noted that information can always be found and are confident it is reliable and trustworthy.

Recommendations

Perform regular testing over the management controls to ensure the integrity, accessibility and usability of information is maintained.

TOPIC 14 – Information maintenance and accessibility

Progressing

Summary of findings

The Authority controls the risks to ongoing accessibility and storage of physical information by keeping all physical information offsite in an external storage facility. The Authority holds location registers for physical information. In addition, the Authority has outsourced IT functions and an external EDRMS support service that regularly communicates any systems updates or risks.

During the recent business system update to the EDRMS, staff indicated they monitored whether all documents had migrated to the new system through testing alongside key external parties.

Recommendations

Identify digital continuity needs for digital information. This could be done in conjunction with developing a register of high-value/high-risk information.

TOPIC 15 – Business continuity and recovery

Progressing

Summary of findings

The current Business Continuity Plan (BCP), which was last updated July 2021, provides an overview of IT's responsibilities during a period of business disruption, particularly to perform a damage assessment of IT services and establish a plan for system restoration. The BCP does not specify which systems and information are critical for business operation. However, the Authority is currently updating a separate draft register that lists all critical functions. In addition, the Authority is currently updating its BCP due to a recent organisational change.

The Authority's servers are managed by a third party. No critical information is stored solely in a physical format. Back-ups are performed daily and handled by the third-party provider. However, testing is not conducted regularly.

Recommendations

Ensure the Business Continuity Plan is kept up-to-date and identifies critical information and systems.

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

The Authority has protection and security controls in place for physical and digital information. The Authority uses third-party storage providers for both physical and digital information, which provides protection against unauthorised access, loss, deletion, or destruction. There is currently no testing of the protection and security processes. Digital information is accessible via Authority devices (i.e. laptops) through role-based access controls and is stored with various third-party vendors. Staff are required to have multifactor authentication on their devices, and this is enforced for login when using devices outside the Authority's local network.

The Leadership Team do not receive regular reporting of information protection and security risks. Without regular reporting, the Senior Leadership Team cannot effectively support the Executive Sponsor in remediating any information protection and security risks to the Authority.

Recommendations

Identify protection and security risks to information and regularly report on these to the Senior Leadership Team.

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

The Authority uses metadata to facilitate the management and discovery of information in the EDRMS. Minimum metadata requirements are built into the Authority's EDRMS to facilitate consistent management and information discovery. Some metadata fields are automated, such as dates and audit trails. However, the shared drives do not meet Archives New Zealand's minimum requirements.

Access controls for the EDRMS are restricted for some confidential files and access must be granted from the information manager and EDRMS support inbox.

Staff interviewed suggested that there are restrictions on EDRMS on what digital information they can access and what they cannot. Staff must contact the information owner and the information manager if they wish to gain access outside of their set permissions. Staff are given induction training on how to use the EDRMS and metadata functionality. However, no ongoing or advanced training on the use of metadata and search techniques is available for staff.

Recommendations

Ensure that all information on the Shared Drive is created and captured on appropriate systems that meet Archives New Zealand's minimum metadata requirements.

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

Progressing

Summary of findings

The Authority has a current and approved organisation-specific disposal authority covering all information formats and business functions. The disposal authority was approved in 2013 and is due to expire in 2023. There is no regular review cycle to ensure that the organisation-specific disposal authority reflects business and legislative changes.

Staff interviewed stated that they seek guidance from the information manager on controls for the capture, retention, and disposal of the information under the organisation-wide disposal authority.

Recommendations

Begin the renewal process on the current organisation-specific disposal authority (due to expire in 2023) with Archives New Zealand.

TOPIC 21 – Implementation of disposal decisions

Beginning

Summary of findings

Disposal actions are not routinely carried out for digital information. The staff members interviewed stated that if they want to delete digital information on EDRMS (i.e., they have accidentally created a duplicate file), information is not permanently deleted but rather moved to a waste bin that can be accessed at a later date. Staff seek guidance from the information manager for disposal decisions.

In April 2022, physical information held by the third-party storage facility had been authorised for destruction, prior to this the last destruction was in 2017. Disposal actions are documented in registers. The destruction of physical information is complete and irreversible.

Recommendations

Ensure disposal actions carried out on digital information are completed.

TOPIC 22 – Transfer to Archives New Zealand

Not Applicable

Summary of findings

This topic has been rated as "Not Applicable" as the Authority does not currently hold information that is over 25 years old which is a requirement for transfer.

The Authority (previously named the Commission) was established in 2003 and became an independent Crown Entity (thereafter named the Electricity Authority) in 2010.

Recommendations

Identify information of archival value that is nearing 25 years old and when appropriate apply for a deferral of transfer agreement for these records or arrange the transfer as required.

6. Summary of feedback

With the recent appointment of the Senior Advisor Information Management the Electricity Authority will be developing and implementing a programme of work to address the recommendations made in the report.

Priority will be given to updating the information management strategy that will set out the policy and procedures covering the categories and topics outlined in the audit report.

A training programme will be developed to ensure that staff receive regular refresher training in information management.

Another key area of focus will be working with Archives NZ to develop and approve a new Disposal Authority.

kpmg.com/nz

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

28 July 2022

James Stevenson-Wallace
Chief Executive
Electricity Authority
James.stevenson-wallace@ea.govt.nz

Tēnā koe James

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the Electricity Authority 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. The Executive Sponsor interviews were held with a nominated responsible officer as through personal circumstances the Executive Sponsor was unavailable.

Introduction

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

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

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

Audit findings

In the audit report, the auditor has independently assessed your information maturity against the framework of our IM Maturity Assessment. Prior to the audit, your organisation completed the Maturity Assessment. This provided a self-assessment of IM maturity for your own use and as context for the auditor about your organisation.

Organisations that are assessed as having a maturity level of 'Managing' across all IM topics are broadly meeting the minimum requirements expected by the PRA and Archives' mandatory Information and records management standard. The audit outcome shows the Electricity Authority at the lower end of the IM maturity scale. However, the new staff appointment and the commitment from the organisation shown in Section 6: *Summary of feedback* of the audit report should result in maturity improvement. The organisation's strengths, its EDRMS and its organisation-specific disposal authority, provide a good basis for improvement in other topics with the support of senior management.

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 eight recommendations as identified in the Appendix.

What will happen next

The audit report and this letter will be proactively released on the Archives website shortly. We would be grateful if you would advise of any redactions that your organisation considers are necessary for the release 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, and we will contact your Executive Sponsor shortly in relation to this.

Nāku noa, nā

Stephen Clarke
Chief Archivist Kaipupuri Matua
Archives New Zealand Te Rua Mahara o te Kāwanatanga

Cc Andy Doube, General Manager Market Policy (Executive Sponsor),
andy.doube@ea.govt.nz

APPENDIX

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
Governance	1: IM strategy	*Update the information management strategy following Archives New Zealand's guidance. The strategy should support business needs and strategic direction of the organisation.*	This is a necessary first step to plan and prioritise the improvement programme and understand the resource requirements.
Governance	2: IM policy and processes	*Complete work on the draft Information Management Policy for approval by the Senior Leadership Team.*	This will support understanding of the Authority's IM obligations, roles and responsibilities. This should be supported by ongoing regular training for staff.
Governance	3: Governance arrangements and Executive Sponsor	*Plan and document information management reporting requirements that provide useful and actionable information of the Executive Sponsor and the wider Senior Leadership Team.*	An organisation of 100 FTEs may not need a dedicated IM governance group. However, the organisation should decide where IM best fits and ensure that it is included in the terms of reference for that group and as a regular agenda item. This is especially important to support the uplift of IM maturity.
Self-Monitoring	7: Self-monitoring	*Design and implement regular information management monitoring processes and report findings that provide useful and actionable information to the Executive Sponsor.*	Keeping the Executive Sponsor informed of issues and activity is essential in ensuring that IM improvement is supported from the senior management level.
Capability	8: Capacity and capability	*Ensure that IM capacity and capability requirements are regularly assessed and monitored against business needs.*	This needs particular attention while the maturity uplift is underway. When the IM strategy is completed the accompanying workplan will need resourcing as well as BAU.

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
Creation	10: Creation and capture of information	*Ensure all information on Shared Drives is created and captured on appropriate systems that meet Archives New Zealand minimum metadata requirements.*	As the organisation has an EDRMS the shared drives should be closed to ensure that information is maintained in controlled systems.
Creation	11: High-value/high-risk information	*Identify high-value/high-risk information assets based on the organisation-specific disposal authority.*	This should be done in the context of developing an information asset register, which will inform the review of the organisation-specific disposal authority (Topic 20).
Disposal	20: Current organisation-specific disposal authorities	*Begin the renewal process on the current organisation-specific disposal authority (due to expire in 2023) with Archives New Zealand.*	This would be a useful process to continue which would then enable a disposal plan to be developed and implemented continuously.