KPMG

Public Records Act 2005 Audit Report for the Independent Police Conduct Authority - Mana Whanonga Pirihimana Motuhake

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 Independent Police Conduct Authority (the 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 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 Authority's information and is not to be used for any other purpose or copied, distributed or quoted whether in whole or in part to any other party without KPMG's prior written consent. Other than our responsibility to Archives New Zealand, neither KPMG nor any member or employee of KPMG assumes any responsibility, or liability of any kind, to any third party in connection with the provision of this report. Accordingly, any third party choosing to rely on this report does so at their own risk. Additionally, we reserve the right but not the obligation to update our report or to revise the information contained therein because of events and transactions occurring subsequent to the date of this report.

Independence

We are independent of Archives New Zealand in accordance with the independence requirements of the Public Records Act 2005.

Contents

1. Executive summary

The Independent Police Conduct Authority (the Authority) is the body that oversees the conduct of the New Zealand Police. The Authority exists so New Zealand citizens have trust that complaints and incidents involving Police conduct will be fairly and impartially investigated or reviewed.

The Authority creates, captures, and maintains high value digital and physical public records relating to, and including:

- Administrative records detailing participation in conferences with overseas bodies.
- Research projects.
- Monitoring of recommendations made by the Authority.
- Complaint case files.

The Authority s primary method for managing information is a Case Management System (CMS). The CMS was last upgraded in 2019. Most complaints are received and maintained electronically. Shared drives are used for meeting minutes and other general Authority documents. Access to the Shared drives is determined by operational group policies. If complaints are received physically, they will be digitised into the CMS. In addition, a third party storage provider holds all the Authorities physical records.

The Authority employs approximately 40 staff members. The Executive Sponsor is responsible for information management at the Authority. The Executive Sponsor is also the Manager of Corporate. However, there are no dedicated information management staff members. While the Authority does not have a dedicated governance group to oversee information management, the Management Team carries out this function. The Management Team is made up of the General Manager and three related Managers of Investigations, Case Resolution and Corporate. The Board members at the Authority have oversight and are involved in signing off policies.

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	**9**
Managing	**5**
Maturing	
Optimising	

2. Introduction

KPMG was commissioned by Archives New Zealand to undertake an independent audit of the Independent Police Conduct Authority under section 33 of the Public Records Act 2005 (PRA). The audit took place on-site in March 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 Independent Police Conduct Authority including both physical and digital information.

The audit involved reviews of selected documentation, interviews with selected staff, including the Executive Sponsor (who also held the information manager role as part of their wider Corporate Service role), the Information Technology team, 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.

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	●				

Note: Topics 17 and 19 in the Information Management Maturity Assessment are applicable to Local Authorities only and have therefore not been assessed.

5. Audit findings by category and topic

Governance

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

TOPIC 1 – IM strategy

Progressing

Summary of findings

The Authority does not have an information management strategy. Information management is broadly included in the wider business strategy. For example, the business strategy most recently included the Authority's upgrade to its existing system to the CMS in 2019.

The Executive Sponsor expressed that the Authority intends to develop an information management strategy to meet its current and future information management needs. This had not yet been started at the time of the audit.

Recommendations

Develop an information management strategy following Archives New Zealand's guidance. This does not have to be a stand-alone strategy as the Authority is a small organisation.

TOPIC 2 – IM policy and processes

Progressing

Summary of findings

The Authority has a draft information management policy (developed by the Executive Sponsor) which has been reviewed by the General Manager but has yet to be approved by the Board. The Board members at the Authority have oversight and are involved in signing off policies. The Executive Sponsor had a role in developing the policy. When the policy is finalised, it will be distributed to staff. Currently, staff refer to the Independent Police Conduct Authority (IPCA) Human Resources Manual for more general information management guidance.

The draft policy links to relevant legislation, the Archives New Zealand Standard, and other internal policies, such as the Human Resources Manual, Code of Conduct and Privacy Policy. It also outlines the responsibilities of all staff and contractors, with specific responsibilities assigned to the Chair of the Authority, Board Members, General Manager, Executive Sponsor and Managers. The staff members interviewed said they were aware of where to find the IPCA Human Resources Manual and other relevant business unit specific processes for information management.

Information management processes are documented at business unit level and have different processes depending on their function. Information management processes are communicated to staff through induction training or as they learn on the job. A comprehensive guidance document for saving documents is available to staff.

Recommendations

Finalise the draft information management policy and distribute to all staff and contractors.

TOPIC 3 – Governance arrangements and Executive Sponsor

Progressing

Summary of findings

The Authority does not have a dedicated information management governance group. The Management Team undertakes this function. The Executive Sponsor is part of the Management Team and is responsible for providing information management updates. However, the management team does not receive regular reporting on wider information management matters, unless something is relevant to report on.

The Executive Sponsor is aware of their oversight and monitoring role in relation to information management. The Executive Team provides the appropriate support to the Executive Sponsor to address information management needs. However, the Executive Sponsor does not receive regular information management reporting from business unit managers.

Recommendations

Design and implement regular information management reporting that provides useful and actionable information that the Executive Sponsor can provide to the Management Team.

TOPIC 4 – IM integration into business processes

Managing

Summary of findings

Staff interviewed were aware of their responsibilities for managing information within their business area. The requirements for managing information are integrated into core business processes due to the nature and sensitivity of the information the Authority handles. Team managers interviewed were aware of their responsibilities and emphasised the importance of a new starter having a buddy to learn information management processes at the Authority. The induction process covers the importance of good information management responsibilities, which has led to the level of awareness staff and team managers have.

Responsibilities for information management are clearly outlined in the draft information policy. Requirements for managing information are integrated throughout business processes due to the Executive Sponsor's role as the Manager of Corporate. Responsibilities for the Manager of Corporate include oversight of the CMS, and as a result, requirements for information management were incorporated into the upgrade from old CMS to the new CMS in 2019.

Any issues with the management of information which impact the Authority are identified by team managers during sample testing. A sample of files are regularly tested to check if additional information and categorisation is correct. Corrective action required is addressed with staff by their team manager.

Recommendations

In conjunction with *Topic 2 – IM Policy and Processes*, finalise the draft information management policy with the Board and distribute it to all staff to ensure the responsibilities for information management are clearly communicated.

TOPIC 5 – Outsourced functions and collaborative arrangements

Beginning

Summary of findings

The key outsourced functions are for information technology (IT) at the Authority, who administer Dynamics 365 and IT support. We reviewed the two contracts for the outsourced IT function and found that information management or public records requirements were not included. Instead, these contracts had generic references to confidentiality and security of information. In addition, there is no evidence of monitoring taking place over these IT contracts.

The Executive Sponsor is not involved in writing or approving information management sections of contracts for outsourced or collaborative arrangements. We note that outsourcing a business function does not reduce an organisation's responsibility to ensure that all information management requirements are met.

Recommendations

Ensure all future contracts for outsourced functions or collaborative arrangements includes roles and responsibilities for information management (where public records are created). This includes monitoring contracted parties to ensure the requirements are met.

TOPIC 6 – Te Tiriti o Waitangi — Beginning

Summary of findings

The Authority has not investigated if any information held is of importance to Māori. As a result, the Authority has not been able to identify any such information and cannot improve access and use of information to Māori. The Authority have indicated that they may have information of importance to Māori, and they wish to improve maturity in this area. However, as the Authority is subject to section 32 of the IPCA Act 1988 *(Authority and Staff to maintain secrecy)* the ability to increase maturity may be limited.

The draft information management policy contains a mandatory requirement to adhere to the principles of Te Tiriti o Waitangi and specifies that information must be accessible to Māori. However, this requirement has not yet been considered for incorporation into processes. There is limited capacity within the Authority to incorporate and maintain metadata in Te Reo Māori to assist in managing information of importance to Māori.

Recommendations

Undertake an exercise to identify whether any information held by the Authority is of importance to Māori. This will inform the Authority as to whether any further actions are required to appropriately manage this information.

Self-monitoring

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

TOPIC 7 – Self-monitoring — Managing

Summary of findings

The Authority monitors compliance with the PRA and other relevant legislation through its bi-annual Legislative Compliance Report. In addition, compliance with internal processes is monitored regularly through dip testing. Dip testing assesses the quality and effectiveness of investigations from the start, through to the closure of the file. One in ten Category D files (no further action complaint files) are randomly selected on a fortnightly basis. Dip testing is performed by an internal assessor and reported to business unit managers to follow up with staff. This also includes looking at the investigation cases to ensure documents are being stored in the correct file format and follow naming conventions in line with processes. Staff members who create and capture information incorrectly are notified. The staff who have failed to comply with processes and procedures are then sent reminders to address the issues. Reporting of dip test results to the Executive Sponsor is only initiated in response to an incident or exception.

Recommendations

Develop a monitoring and reporting plan for the organisation to address identified information management risks.

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

Beginning

Summary of findings

The Authority has no dedicated information management personnel other than the Executive Sponsor. The Executive Sponsor has access to information related professional development opportunities if requested.

Staff interviewed reported that they are supported by the Executive Sponsor for information management needs. However, the Authority acknowledges that it has limited capacity to meet its information management needs effectively. There are ongoing conversations to identify how to best address this, but to date there is no formal plan to evaluate information management capacity against business needs. However, the Authority noted that they are restricted by budget.

Recommendations

Assess what information management resources are required to support the Authority's needs. These could be supported by internal staff or by a contracted resource to consider information management requirements are appropriately addressed.

TOPIC 9 – IM roles and responsibilities

Progressing

Summary of findings

The staff members interviewed understand their information management responsibilities and the specific requirements in relation to their role. While these responsibilities are documented in job descriptions for some roles (e.g., the General Manager), they are not documented for all staff.

Staff receive a formal induction to the Authority, which includes information management. As part of this process, new staff receive an induction pack (IPCA Human Resources Manual) containing information management guidance alongside other internal policies and procedural documents. New starters are provided with a mentor to assist with general questions including information management matters.

There is no regular information management training provided to staff or contractors. However, the staff members interviewed were comfortable reaching out to the Executive Sponsor or their relevant business manager if they needed information management support. In addition, organisation-wide information management notices are sent via email to communicate process changes and policy updates.

Recommendations

Ensure job descriptions and performance plans document information management roles and responsibilities for 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. Staff at the Authority actively ensure that the right information is routinely created and captured as part of all business functions and activities. Due to the sensitive nature of the information, the Authority actively discourages the use of uncontrolled environments to manage information.

The Authority currently meets Archives New Zealand's minimum metadata requirements for information stored on the CMS.

Shared drives (R Drive) are used for operational documentation such as storing internal supporting documents. The shared drives do not meet minimum metadata requirements. All case material is saved exclusively on the CMS. Access to the R drive to create or capture information is determined by the group access policy.

Staff consider records to be reliable and trustworthy. There is a structured approach to monitoring and addressing information usability and reliability issues through dip testing. If there are any issues identified by an internal assessor performing the testing, business unit managers would actively follow up with staff.

Recommendations

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

TOPIC 11 – High-value / high-risk information

Progressing

Summary of findings

The Authority has multiple registers that detail the inventory of physical and digital information held. The Authority has a high-level awareness of what information they hold that could be considered high-value or high-risk. For example, complaint reports that are Category A (independent investigations) are considered high value.

The Authority maintains the following registers:

- Assets register for physical information held off-site. This register details information by year.
- Category A register (IPCA independent investigation).
- A register of public report index which details publicly available reports.

There is no process in place to ensure the asset registers are routinely updated.

Recommendations

Create a process to ensure registers kept by the Authority are maintained and kept current. The process should also include the ongoing review of the risks to the high-value/high-risk information kept on the register.

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

The Executive Sponsor is involved in the design and configuration of new and upgraded business systems, such as the upgrade to the new CMS in 2019. Design specifications and requirements were considered as part of this upgrade. The CMS database captures the minimum metadata requirements set out by Archives New Zealand.

As part of the Executive Sponsor's corporate management duties, they are involved in project work and ensuring information management is considered as part of any business change. However, no standardised information management requirements for new and upgraded business systems are documented.

Recommendations

Create standardised information management requirements for new and upgraded business systems and ensure information management expertise is included as part of this process. This can be included in the Authority's information management policy in conjunction with *Topic 2 – IM policy and processes*.

TOPIC 13 – Integrity of information

Managing

Summary of findings

The Authority has localised business unit (i.e., case management team) information practices in place that are routinely followed by staff. Information practices are in place to ensure that information is reliable and trustworthy.

Management controls are in place to maintain the accessibility and integrity of information in the CMS, including descriptive metadata, file naming conventions and automatic audit trails. These are routinely tested and followed up with staff through dip testing. Dip testing also ensures that the information is comprehensive and complete.

Staff are aware of the Authority's advanced search tool to find and retrieve information, and it contains optimised filtering functions to ensure all information is highly accessible. Staff are confident that all information held in the CMS comprehensive and complete.

Recommendations

Review localised processes to ensure information management practises are consistent across the organisation.

TOPIC 14 – Information maintenance and accessibility

Progressing

Summary of findings

The Authority has tools to help manage and maintain physical information during business change. For example, there are processes to assess risk during service upgrades and regular checks when the systems are back online. Regular testing is also performed prior to and postproduction. File migration and monitoring was performed during the upgrade to the new CMS in 2019.

The Authority has not assessed the risk of technology obsolescence and preservation of physical of information.

The Authority is aware of the need to digitise historic physical information held offsite to ensure it remains accessible. The Authority is subject to budget constraints, therefore has not addressed this risk of inaccessibility. The Authority also hold floppy disks and DVDs which are at risk of obsolescence.

Access controls are in place in the CMS, such that some files that are confidential have stricter controls depending on the confidentiality of the information. Access to information on the R-drive can be accessed dependent on operational group policies determined by the Active Directory permissions and access.

Recommendations

Complete a risk assessment to identify information that is at risk of obsolescence for information stored on both the CMS and R-drive and develop a plan to manage this risk.

TOPIC 15 – Business continuity and recovery

Beginning

Summary of findings

The Authority does not have a current and approved business continuity plan. A draft plan is currently waiting for formal approval and distribution.

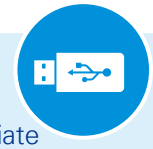
The Authority has identified the risks to digital information in the draft plan and has detailed actions for the restoration of digital business information. Data back-up processes, computer and business systems and temporary alternate technologies are also identified in the draft plan.

The Executive Sponsor has sought approval from relevant third parties regarding cyber-attack mitigation strategies and continues to assess solutions and response functions.

No critical information is stored solely in physical format which would delay business as usual operations. The outsourced IT function understand what information is critical and regularly test back-ups to ensure it can be retrieved if necessary.

Recommendations

Prioritise formally approving the business continuity plan.



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

Managing

Summary of findings

The Authority uses third-party storage providers for both physical and digital information, which provides protection against the unauthorised access, loss, deletion, or destruction.

Physical information is predominantly stored offsite with a third-party storage provider. The Authority noted they no longer receive a large amount of physical information. This will be digitised if received in physical form to the relevant case on the CMS.

Digital information is stored with approved cloud providers and on a server in Christchurch. Data is accessible based on permissions set by the Case Management Team in the CMS. For example, some cases are restricted to specific permissions depending on whether the staff member is responsible for resolving the case.

Information protection and security risks are regularly reported to the Executive Sponsor. These are provided by both outsourced IT functions. The Executive Sponsor will report any issues to the General Manager and Chair of the Authority on an as needed basis.

Recommendations

Regularly report information protection and security risks to the Management Team and determine remediation actions.

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 CMS. The CMS requires that certain metadata fields are input during the creation of the documents. Some metadata fields are automated such as dates and audit trails, however, most filing conventions are input manually. The CMS meets the Archives New Zealand minimum requirements. The shared drives (R Drive) do not meet Archives New Zealand minimum requirements.

The Authority consistently uses descriptive file plans and metadata schema to facilitate consistent management and discovery of information. This is included in the guidance documents, which illustrates how cases should be saved and the comprehensive metadata required in the CMS. Although there is an induction process in place for all staff, there is no regular advanced training in the use of metadata and search techniques.

Access control documents are set at business unit level within the CMS. All staff have the same operational access privileges except for restricted access investigations, which are determined by a case-by-case basis. Access controls for the building are protected by swipe card, and there is dual authentication required for access to some systems. Access to shared drives (R Drive) is determined by operational group policies determined by the Active Directory permissions and access.

Recommendations

Ensure all information is created and captured on appropriate systems that meet Archives New Zealand 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

Managing

Summary of findings

The Authority has a current and approved organisation-specific disposal authority covering all formats and business functions. The disposal authority was approved in 2013 and is current to 2023. There has been regular review with Archives in 2014 and 2018 for updates to ensure information reflects business and legislative change.

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

No recent disposal decisions have been taken against physical or digital records. During the 2019 migration to the new CMS, no disposal decisions took place. In addition, physical documents held in storage are not regularly reviewed for disposal.

The Authority does not have a plan to regularly monitor and manage information to enable regular disposal decisions to be made. Rather, information is retained indefinitely. This poses the risk that the Authority will be holding on to records for longer than they need to.

The Executive Sponsor understands their records must be retained for a minimum period under their approved disposal authority. However, it was identified that more resourcing is required to review older content to identify what may be disposed of under the disposal authority.

Recommendations

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

TOPIC 22 – Transfer to Archives New Zealand

Beginning

Summary of findings

The Authority was established in 1988 and is required to identify all information of archival value which is over 25 years old. A register identifies all the files maintained that are over 25 years old with archival value. The Authority does not currently have a deferral of transfer agreement in place with Archives New Zealand. The Authority also noted that it is a challenge for them as some files need to be retained for 50 years (Category A and B complaints).

Recommendations

Apply for a deferral of transfer agreement or transfer appropriate records to Archives New Zealand.

6. Summary of feedback

Acknowledgement

Mana Whanoga Pirihimana Motuhake, the Independent Police Conduct Authority has found the Public Records Act Audit of its Information Management practices to be a hugely beneficial exercise, it has afforded the Authority the opportunity to pause and focus on this vital area of our organisational capability.

On behalf of the IPCA, we thank the staff from KPMG for engaging with our staff in such a positive and constructive way, we have gained many valuable insights that will help us develop our capability in this area.

Commentary

As with many smaller organisations facing the challenge of increasing compliance obligations, a restrictive baseline funding model, and the ongoing need to prioritise investment towards our core operational activities, (especially the attraction and retention of operational personnel) the Authority acknowledges a severe limitation in the application of dedicated resourcing to its back-office functions and HR roles dedicated to carrying out and developing our information management practices.

However, we have a very supportive Board who have a strong vision for the future Authority, including our information management capability. We are currently revising and documenting the information management strategy in tandem with our broader operational strategy. Some of the material available to the Audit team was in draft, as it was under review, and/or is being updated to reflect the robust information management practices in place, but for reasons of limited time and resource, has yet to be approved as a finalised document.

Prioritised Activity

Our prioritized activities in response to the Audit recommendations focus on the finalisation and formalisation of our current information management documentation, monitoring, and reporting.

Information Management Strategy and Policy

Draft documents are to be finalised and approved by Board, following which the documents will be circulated to all Authority staff to provide specific 'cross-organisation' information management guidance alongside the existing broader operational guidelines and policy documents.

Information Management Governance Group, Annual Information Management work plan, and Information Management Reporting framework.

Activities already being undertaken on an ad hoc basis will be developed, and where necessary expanded to occur within a regular and formalised framework to ensure that appropriate monitoring and reporting is occurring on a regular basis so that identified information management risks can be dealt with in a more responsive way and receive earlier targeted resource allocations.

Creation and Capture of information

The Authority is currently undertaking a programme of works that will update the platforms within which ALL business information is created and held, this will see the retirement of any remaining legacy platforms, including the Shared R: Drive referenced in the Audit.

Te Tiriti o Waitangi

The Audit has highlighted the need for the Authority to take a high-level review of all information it receives, to assess what information is of specific importance to Māori, thereafter, applying a te Ao Māori lens to the appropriate manner in which that information should be captured, held, and accessed. Undertaking this exercise, will have help inform and develop other aspects of Authority's organisational capability, including the development of our engagement strategy and partnership with Māori and Iwi community.

Concluding

In conjunction with these prioritised activities we have also collated the remaining recommendations into a schedule of works that has identified other aspects of our information management practices that should be addressed as and when they arise, these activities can be incorporated into our BAU activities, such as including review of information management requirements when undertaking regular review or renewal of service contracts and agreements, future system development and expansion, and training opportunities for all of our staff so that an information management culture prevails across all of our business activities.

kpmg.com/nz

Te Rua Mahara o te Kāwanatanga
ARCHIVES NEW ZEALAND

23 June 2022

Archives New Zealand, 10 Mulgrave Street, Wellington
Phone +64 499 5595
Websites www.archives.govt.nz
www.dia.govt.nz

Judge Colin Doherty
Chair of the Authority
Independent Police Conduct Authority
admin.services@ipca.govt.nz

Tēnā koe Judge Doherty

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the Independent Police Conduct 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.

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 Authority is mostly operating at the 'Progressing' maturity level with some topics in the 'Managing' level.

The very positive engagement of the Authority with the audit process and outcome is clear from the audit report Section 6: *Summary of feedback.* Improvement work has already been prioritised within the resourcing available for your small organisation. The completion of the IM strategy will further clarify ongoing resourcing requirements. The Authority may need to source external IM advice to enable improvement in some topics.

Prioritised recommendations

The audit report lists 19 recommendations to improve your organisation's IM maturity.

We endorse all recommendations as appropriate and relevant. To focus your IM improvement programme, we consider that your organisation should prioritise the seven recommendations as identified in the Appendix.

What will happen next

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

Honiana Love
Acting Chief Archivist Kaipupuri Matua
Archives New Zealand Te Rua Mahara o te Kāwanatanga

Cc Julie Beijen, Manager, Corporate. julie.beijen@ipca.govt.nz (Executive Sponsor)

APPENDIX

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
Governance	1: IM strategy	*Develop an information management strategy following Archives New Zealand's guidance. This does not have to be a stand-alone strategy as the Authority is a small organistion.*	This is key in prioritising investment to support maturity improvement and to understand the ongoing resourcing requirements.
Governance	2: IM policy and processes	*Finalise the draft information management policy and distribute to all staff and contractors.*	This will be of benefit across the organisation and help lift maturity in other topics. Formalising IM induction would also help to ensure consistent understanding and practice across the organisation.
Governance	3: Governance arrangements and Executive Sponsor	*Design and implement regular information management reporting that provides useful and actionable information that the Executive Sponsor can provide to the Management Team.*	An example of what could be included in regular reporting is the sampling of files described in Topic 4: *IM integration into business processes* and Topic 7: *Self-monitoring.*
Governance	6: Te Tiriti o Waitangi	*Undertake an exercise to identify whether any information held by the Authority is of importance to Māori. This will inform the Authority as to whether any further actions are required to appropriately manage this information.*	The Authority should note the guidance provided by Te Arawhiti to support building capability to meaningfully engage with Māori.
Capability	8: Capacity and capability	*Assess what information management resources are required to support the Authority's needs. These could be supported by internal staff or by a contracted resource to consider information management requirements are appropriately addressed.*	The organisation-specific disposal authority expires in 2023 and will require significant resourcing. This needs to be taken into consideration - see Topic 20: *Current organisation-specific disposal authorities.* The summary of findings for Topic 21: *Implementation of disposal decisions* also identifies the need for more resource to implement disposal.

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
Creation	10: Creation and capture of information	*Ensure all information is created and captured on appropriate systems that meet Archives New Zealand minimum metadata requirements.*	This recommendation refers to the use of the shared R network drive which does not meet metadata requirements. Control of this environment is limited which puts the information stored there at risk.
Disposal	21: Implementation of disposal decisions	*Develop a disposal implementation plan and assess the resources necessary to perform disposal actions.*	The Authority is well placed to start this work with its current organisation-specific disposal authority. Disposal will also help mitigate risks in retaining information longer than is required.