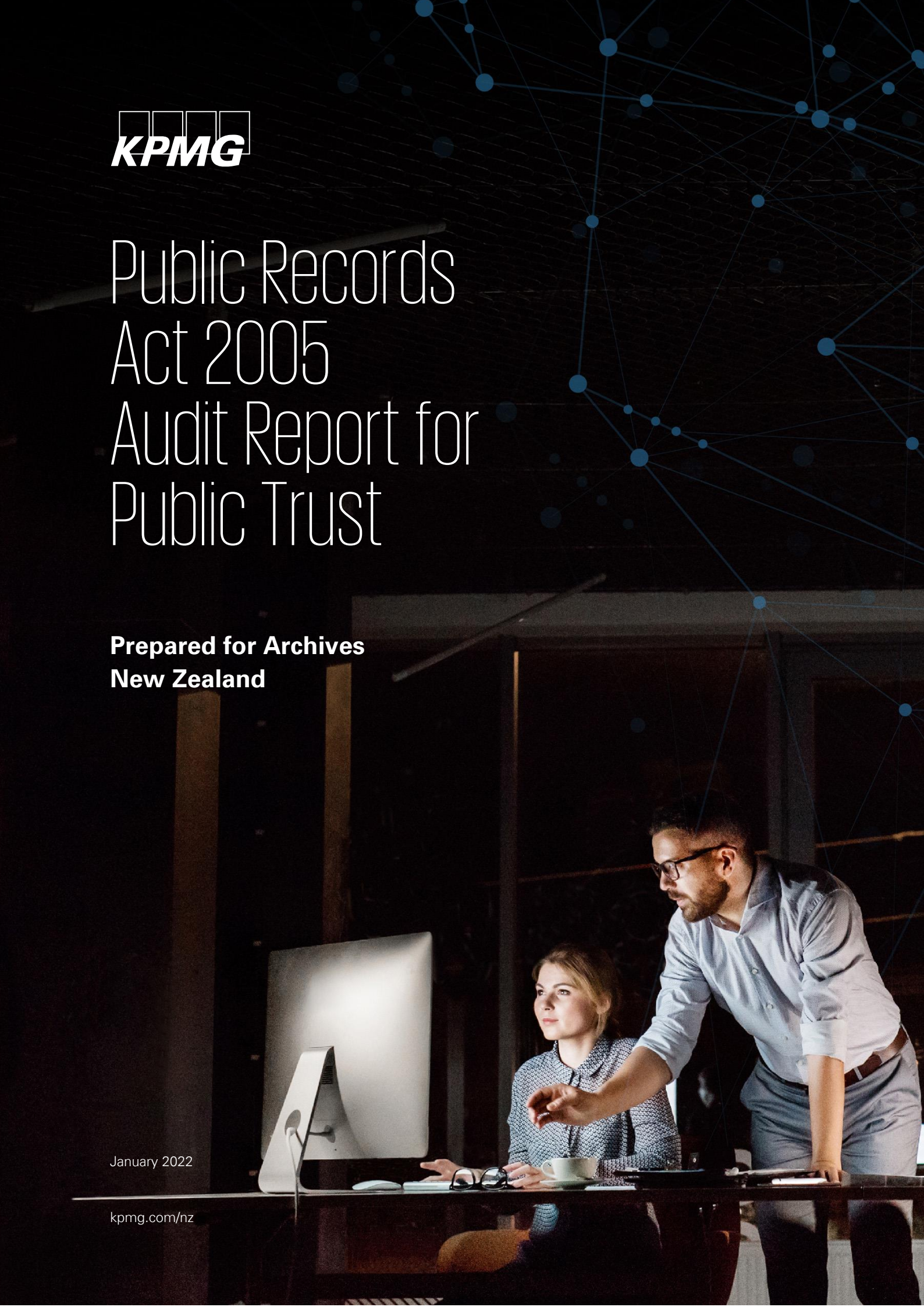
KPMG

Public Records Act 2005 Audit Report for Public Trust

Prepared for Archives New Zealand



January 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 Public Trust. We have indicated within this report the sources of the information provided. Unless otherwise stated in this report, we have relied upon the truth, accuracy and completeness of any information provided or made available to us in connection with the Services without independently verifying it.

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 Public Trust 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 Public Trust'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.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Contents

1. Executive summary

Public Trust (PT) is the largest provider of Wills and Estate administration services in New Zealand. PT creates high value public records, including wills, enduring powers of attorney, trust deeds and details of people's assets.

PT has an Enterprise Content Management system (ECM) and a Document Management tool (DMS). Staff also have access to and use network drives. PT has recently migrated to Office 365.

Records are maintained electronically and physically, with hard copy files stored onsite and offsite at a commercial storage facility. There is work underway to digitise some physical information.

There are currently no dedicated information management resources at PT. However, PT intends to recruit for an information management position in 2022. In total, there are 415 FTE across 27 regional offices.

Following a review completed by a third party contractor in early 2021, PT started working towards building and establishing information management capability associated strategies and processes. This is expected to be rolled out in early 2022.

PT'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	**17**
Progressing	**3**
Managing	**0**
Maturing	**0**
Optimising	**0**

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2. Introduction

KPMG was commissioned by Archives New Zealand to undertake an independent audit of Public Trust (PT) under section 33 of the Public Records Act 2005 (PRA). The audit took place in December 2021.

PT'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 PT including both physical and digital information.

The audit involved reviews of selected documentation, interviews with selected staff, including the Executive Sponsor, the Information Technology team, and a sample of other staff members from various areas of the organisation. Note that the Executive Sponsor is the senior responsible officer for the audit.

The audit reviewed PT'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. PT has reviewed the draft report, and a summary of their comments can be found in section 6.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

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.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

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

PT does not have an information management strategy to provide strategic direction and support over information management activities. However, an active work program is underway to develop and implement an organisation-wide information strategy in 2022.

There is considerable top-level support from senior stakeholders at PT for information management. This is evident through recent investments to improve this area, such as the formation of an information management governance group (refer to Topic 3 – *Governance arrangements and Executive Sponsor)*.

Recommendations

Complete the work programme to develop the information strategy. The information management strategy should be approved by senior management, communicated to all staff and contractors, and reviewed on a periodic basis to ensure it continues to align with PT's business activity.

TOPIC 2 – IM policy and processes — Beginning

Summary of findings

PT does not have a formal information management policy or associated processes. As a result, roles and responsibilities for information management have not been identified or defined. This has led to an inconsistent approach to information management across the organisation. PT plans to develop both the policy and roles and responsibilities alongside the information management strategy in 2022.

The staff interviewed had a general awareness of information management processes for their individual business unit which was gained through shadowing senior team members, buddies, or experience. Although some information management processes are documented, they are not extensive, nor are they dated, making it difficult to determine their relevance.

PT staff have a strong understanding of responsibilities and requirements under the Official Information Act and the Privacy Act. However, their knowledge is limited when it comes to the Public Records Act. Senior staff place a strong expectation on their teams to understand the importance of the information they are handling and the individual process to capture it within their corresponding business units.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Recommendations

Deliver the work program to implement an information management policy and associated process documents that provide formal information management guidance to staff. The policy should support the information management strategy (refer to Topic 1 - *IM Strategy*). It should include roles and responsibilities, align to the Archives New Zealand standard and requirements, and relevant legislation.

Communicate the policy to all staff and contractors and review on a periodic basis to ensure it continues to align with PT's business activity.

TOPIC 3 – Governance arrangements and Executive Sponsor — Beginning

Summary of findings

The Executive Sponsor is aware of their oversight and monitoring role, and currently fulfils this through the development of the information management work program. There is no regular or formal reporting of information management activities to the Executive Sponsor as the work program is in development. However, because the outputs of the work program have not yet been implemented, regular reporting will not commence until 2022.

PT has established a governance group that covers information management. This group was established to drive information management initiatives and projects that will be implemented in 2022. This group is largely comprised of senior stakeholders and representatives from each business group to ensure a whole-of-organisation approach. The Executive Sponsor is the lead of the information management governance group and has acquired significant support from the ELT and Board as a result of active communication maintained between the parties, led by the Executive Sponsor.

Recommendations

Design reporting that provides useful and actionable information for the Executive Sponsor. Establish and formalise regular reporting once strategies and policies are established at PT.

TOPIC 4 – IM integration into business processes — Beginning

Summary of findings

Information management is not explicitly integrated into business processes and activities organisation-wide. As a result, there is a fragmented approach across PT, meaning approaches to information management are dependent on each business group.

Expectations on some facets of information management are communicated to staff members, such as ensuring information is filed in the appropriate location. However, there is an inconsistent approach to naming conventions across PT, resulting in difficulty finding information on business systems.

Responsibility for managing information within business units is inconsistently assigned to business owners.

Recommendations

Assign and document responsibility for creating and managing information in business processes to business owners.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

TOPIC 5 – Outsourced functions and collaborative arrangements

Beginning

Summary of findings

PT is not aware of any significant outsourced functions or collaborative arrangements in place. Based on the sample of contracts we reviewed with third parties, there was no recognition of the public records status of information held by them.

The contract with the third-party contractor was also reviewed. This included specific clauses on confidentiality, privacy, roles and responsibilities and specified that PT had sole and exclusive ownership of all intellectual property rights to their information. However, the clauses made no reference to the Public Records Act or the public records status of the deliverables.

Recommendations

Going forward, if PT outsources a business function or enters into a collaborative agreement that will result in the creation, maintenance and disposal of PT's records, information management requirements should be standardised and included in these contracts.

TOPIC 6 – Te Tiriti o Waitangi

Beginning

Summary of findings

Information of importance to Māori has not been identified. Information management implications within Te Tiriti o Waitangi settlement agreements and other agreements with Māori are not known.

PT acknowledges that it is at the beginning of its journey and are keen to understand their obligations under the Treaty. However, PT note there is confusion/complexity to understanding what its obligations are due to the nature of being both a Crown Entity and having to operate as an effective commercial business.

Recommendations

Undertake an exercise in consultation with external Māori groups and iwi to identify and assess whether there is information of importance to Māori that PT holds. The outcome of this exercise will inform PT 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

There is no regular, formal monitoring of information management, due to there being no established policy or process in place. Instead, issues around information management are discussed within the teams on an informal, as required basis.

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

There are four to five internal audits carried out every financial year, covering a range of topics. We noted that PT currently have approximately 15 specific findings relating to information management. Action items for these were either in progress or awaiting approval. However, the audits performed were not specifically focussed on information management at PT, but on business areas that had been prioritised by the PT Board, which happened to have an information management element. Findings were communicated to the managers accountable for the areas audited and plans are created by them to address findings.

Recommendations

Design regular information management monitoring procedures and report the findings that provide useful and actionable information to the Senior Leadership Team and the Executive Sponsor. This should be actioned following the completion of the recommendations outlined in Topic 2 – *IM Policy and Processes.*

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

There is limited access to appropriate information management capability. However, PT has commenced work to address internal information management capability and capacity requirements. PT intends to recruit for one FTE position specifically focused on information management in 2022. At present, PT is supported by a third party to understand information management requirements.

The Executive Sponsor noted a desire to establish an information management champion network internally at PT, with representatives from each business group. Each champion selected would be provided with appropriate information management training to support their role. This is to ensure sole reliance does not rest with the information management position and that each business group remains accountable for information management requirements. This is an opportunity PT will explore further once it has appointed the information management role.

Recommendations

Assess information management capability and capacity requirements against business needs and consider training opportunities for information management champions to support the Executive Sponsor and the information management role once appointed.

TOPIC 9 – IM roles and responsibilities

Beginning

Summary of findings

PT's staff have general awareness of their information management responsibilities. However, as policies and processes are not documented, understanding information management responsibilities is primarily due to staff involvement in all aspects of operations and the need to manage information appropriately for day-to-day activities.

There is no formal information management training provided to staff across PT. While staff members in the Retail business group receive training regarding the systems they use and some legislative obligations, the training does not comprehensively cover information management. Staff members in other business groups mentioned that they

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

learned the information management practices necessary for their role from on-the-job training, buddying with colleagues and from their managers.

Roles and responsibilities for information management are not documented in job descriptions, performance plans and codes of conduct for staff and contractors, so they are not assessed as part of employee performance. Employment agreements include a statement outlining that compliance with PT policies is required. However, as PT does not have an up-to-date information management policy, this requirement does not sufficiently cover information management.

Recommendations

Include information management roles and responsibilities for staff and contractors in job descriptions and PT's code of conduct.

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 — Beginning

Summary of findings

Information is created and captured in an ad hoc way and is dependent on practices within each business group. Each business group is aware of what information they need to create and capture and the appropriate system to do this. However, these approaches are linked to compliance with other legislative obligations rather than the Public Records Act and the Information and Records Management Standard.

Some information is created and captured in uncontrolled environments. Working drafts of documents are saved and used in either personal drives, H:Drive, or in Microsoft Teams. Some staff also acknowledged using emails as a way of capturing information. The expectation at PT is that all final versions of documents created are filed in the appropriate business system. To avoid loss of information and records, PT's ICT team noted recent system updates mean that all information stored across PT systems and network drives is backed up. This includes automated email archiving, One Drive linked to business drives, and migration to MS365.

Appropriate metadata is not created to support the usability, reliability and trustworthiness of the information. The functionality to create metadata exists in a PT business system, however, it is manual and not mandatory for staff to fill in the metadata. In another business system, staff are able to find an overarching client file, but have difficulty in retrieving an exact document. One staff member noted that version control varies across the systems, for example, if 15 versions of a document exist, it is difficult to determine which document is the most recent one and may require the staff member to review each one. In addition, some staff still use an old system to search for client-related documents as it is easier and quicker to find them than current systems. The search results from the older system often enables PT staff to find the appropriate document/ file in the appropriate system.

Recommendations

Identify and address information usability, reliability and trust issues.

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

TOPIC 11 – High-value / high-risk information

Beginning

Summary of findings

There is an understanding of what information may be considered high-value or high-risk across PT and the importance of this information to its clients. However, there is no formal identification or management plan currently in place for the high-value or high-risk information assets it maintains.

PT holds millions of individual records, with over three million records in the document management tool alone. Creating an information asset register of high-value or high-risk information assets would enable PT to group this data together and 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 PT.

PT is currently assessing data classification frameworks to implement that could help streamline its information and records.

Recommendations

Define what information is considered high-value or high-risk to PT.

Create an information asset register that identifies the information that is high-value or high-risk to PT and develop a plan for the long-term management of this information across the organisation.

Management

Management of information should be designed into systems to ensure its ongoing management and access over time, including following a business disruption event. Information must be reliable, trustworthy and complete and managed to ensure it is easy to find, retrieve and use, as well as protected and secure.

TOPIC 12 – IM requirements built into technology systems

Beginning

Summary of findings

Information management requirements are generally not addressed in the design and configuration of the upgraded business systems but are for new systems. A third-party contractor supports PT's understanding of its information management requirements. This has helped inform future work programmes focussed on information management, such as the data classification framework.

Current business systems used to capture and maintain digital records have the ability and underlying design capability to capture metadata. However, PT does not have metadata requirements defined or consistently implemented so that the minimum metadata required by Archives New Zealand is captured. We note that MS365 meets these requirements but as PT have only recently migrated to MS365, the additional metadata will not improve findability for existing information or information stored on other systems.

Recommendations

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

Ensure that information management requirements are considered throughout the development and improvement of all new and existing business systems, including minimum metadata requirements where applicable.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

TOPIC 13 – Integrity of information

Progressing

Summary of findings

Information management practices are based on localised approaches driven by individual business groups. There is no blanket / consistent approach to information management. For example, the Retail business group has a filing structure where documents are saved using the same folder structure for all customers in the ECM. Similar practices are not employed consistently by other business groups and for other systems.

Staff provided examples of variable experiences when trying to find and retrieve information within systems. They were not always confident that the information was comprehensive and complete, often having to look through other documents in case there was another more complete version. While they could locate all files relating to a customer within the ECM, they sometimes had difficulty finding the specific file they were searching for due to the sheer number of files. This could be due to the lack of a formal, documented naming convention. The number of systems in use also means that it takes new joiners some time to understand what kinds of information are stored in each system. Also, finding historic information presented some difficulties at times due to the location of the file or the names given to the files.

Recommendations

Define and implement standardised information processes across PT's business groups to ensure consistency.

TOPIC 14 – Information maintenance and accessibility

Beginning

Summary of findings

There are no formal strategies to manage and maintain physical or digital information during business and system changes. As noted, there is a fragmented approach to information management across PT. Practices to manage and maintain information at PT are mainly undocumented and dependent on each business group.

Ongoing accessibility risks to digital information are not identified. PT does not delete information, and there is a strong reliance on backups to protect digital information. When information is moved/migrated between systems, it remains with PT's network and data centres. This enables PT to control and secure its data easily. A full reconciliation of data is completed post transit to ensure continued accessibility to PT information.

Accessibility risks have not been formally recorded nor associated with any mitigating controls.

Some risks to the ongoing accessibility of physical information are identified. These are recorded in the online hazards register, which is maintained and reviewed weekly by the PT Risk team.

Preservation needs for either physical or digital information have not been identified. It is intended this will be an element of PT's future information management roadmap.

Recommendations

Identify preservation needs for both physical and digital information kept by PT.

Establish a formal and periodic review of ongoing accessibility and preservation needs for physical and digital information. The information management asset register (see Topic 11 – *High-value/high risk information*) should support this review.

TOPIC 15 – Business continuity and recovery

Progressing

Summary of findings

PT has multiple BCPs, each tailored to critical business functions or location or the type of scenario that affects business continuity. We reviewed three of these, the Technology and Digital Business Continuity Plans and the

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

External Risk BCP. All three have been updated in 2021. They identify the critical core systems and include the actions for the restoration of digital business information. However, the business continuity plans do not identify the critical information required to continue operating during a business disruption, nor do they cover the restoration of physical business information.

Digital information is backed up daily, weekly, monthly and annually, with retention ranging up to seven years. We note that ECM back-ups should be used solely for disaster recovery purposes and not as a long-term retention of records strategy, and ideally, should only be kept for a period of two years. Long-term retention of ECM back-ups creates additional risk for PT, including the risk of use of outdated information.

PT has performed ad-hoc backup recoveries of digital data on a small scale, such as individual emails, with no issues noted. An annual disaster recovery test is performed that shows whether data backed-up from systems can be recovered.

Recommendations

Ensure that the identification of critical systems in the BCP includes identification of the critical information required to ensure business continuity following a disruption.

Develop a plan for the salvage and restoration of physical business information, particularly wills and trusts.

Back-up processes should also be re-designed for solely disaster recovery purposes, with back-ups retained for no more than two years.

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

There is protection and security for some physical information against unauthorised access, loss or destruction although these measures are not regularly tested. For example, physical wills are usually secured in a locked, fireproof room accessible to only one team at each office. Other physical files are stored in unlocked file cabinets, located in the same area as the relevant team the files relate to. There is reliance on staff to remain vigilant that files are not inappropriately accessed by staff in other business groups/teams. However, each floor or regional office has access control arrangements. Physical files stored offsite at a third-party storage facility have a Do Not Destroy order against them.

There is appropriate protection and security for digital information against unauthorised access, loss, deletion, or destruction (including third-party storage providers and in transit). This is evident in the various controls in place, for example, there are user access controls across all business systems and drives, and the ability to delete information is limited to a small number of staff members. Even so, this is limited to a soft delete.

Hazards that may impact the information storage environment for both digital and physical information have been identified. These are recorded and maintained in an online hazards register monitored by the PT Risk team.

The storage environment for physical information has some physical protection against hazards, for example, floods or fires. The secured wills room inspected is fireproof and has sprinklers located in the room. Other centres have a combination of fire proofing / sprinkler protection, though there is not a consistent standard of both across all centres.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Recommendations

Regularly report information protection and security risks to PT's information management governance group and identify 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

Beginning

Summary of findings

PT takes a decentralised approach to information management where each business group is responsible for maintaining information on the systems they use. This means that the accessibility of information varies depending on the system that the information is stored in. Staff interviewed were knowledgeable on how to use PT's business and information systems as this is covered as part of their onboarding or ongoing on-the-job training.

Where staff require information from other business groups, the differing information management approaches can slow the process of accessing required files, as staff are sometimes reliant on their colleagues sourcing the information on their behalf. In addition, the majority of systems used (network drives and ECM) are not designed to create and maintain minimum metadata required by Archives New Zealand. Where staff identify information management issues, they seek guidance from or escalate to their line managers or the IT support desk.

Access to information is controlled by restricted access to systems. For example, there are access controls within the ECM that limit staff from accessing information that is not relevant to their roles. Staff interviewed confirmed that they have adequate access to systems to find and use the information they need. They could request the ICT team for access at any time. Information sharing with external parties is primarily done through email and secure file transfer protocol (SFTP). USB ports to PT systems are locked, and staff would need to liaise with the ICT team to transfer information to a USB.

Recommendations

Identify the issues around inconsistent management of information in systems and develop a plan to improve information findability.

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".

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

TOPIC 20 – Current organisation-specific disposal authorities

Beginning

Summary of findings

There is no current, approved organisation-specific disposal authority. PT have never had an organisation-specific disposal authority.

Recommendations

Prioritise the development of an organisation-specific disposal authority that covers all formats and business functions that is approved by Archives New Zealand.

TOPIC 21 – Implementation of disposal decisions

Beginning

Summary of findings

No digital or physical records have been disposed of in the recent past, except for paper-based correspondence that has been digitised. PT does not have an organisation-specific general disposal authority, therefore are restricted from disposing of physical and/or digital documents.

There are no formal plans to dispose of physical or digital information, and no processes are currently in place to identify information that can be disposed of under the General Disposal Authorities. PT takes a conservative approach towards the disposal of information. However, this poses the risk that PT will be holding on to records for longer than they need to.

Recommendations

Create a plan to regularly carry out disposal decisions once the organisation-specific disposal authority has been created and approved (refer to Topic 20 – *Current organisation-specific disposal authorities*)

TOPIC 22 – Transfer to Archives New Zealand

Beginning

Summary of findings

Physical and digital information of archival value that is over 25 years old has not been identified or determined as open or restricted access. PT is aware of the requirement that records older than 25 years should be transferred to Archives New Zealand, however, have not actioned this transfer due to the volume of records kept by PT and lack of an organisation-specific disposal authority.

Recommendations

Following approval of the organisation-specific disposal authority, identify information due for transfer to Archives New Zealand. Either transfer or apply for deferral of transfer.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

6. Summary of feedback

Thank you for the opportunity to participate in the Public Records Act 2005 audit. In mid-late 2021, Public Trust engaged a third party, Maven Consulting to better understand our information management capability and maturity, by undertaking an extensive review of our information management practices and processes. This work provided Public Trust a solid understanding of our current information management maturity, which has been reinforced by the findings of Archives New Zealand in this audit.

Public Trust's focus has now shifted to increasing our capability and maturity, utilising the findings from our 2021 review and incorporating the recommendations from the Archives NZ Audit.

Aspects of this work have already commenced with the establishment of an Information Management Governance Team, our transition to M365 and work to create a data classification framework. From here Public Trust is committed to creating an Information Management Strategy and ensuring our information management policies and processes are well documented and embedded. Although this foundational work needs to be prioritised, Public Trust is of the view that a number of other recommendations from the audit will be able to commence in parallel, with an aim to make tangible progress in uplifting our maturity throughout 2022.

Information maturity uplift will be a multi-year programme of work for Public Trust, and a pragmatic approach will need to be taken about the pace at which maturity can be increased, having regard to organisational capacity and resources. Despite this, Public Trust recognises the benefits of more mature information management practices and is committed to an uplift in maturity over the coming years.

Public Trust notes that the vast majority of its information is client information, being the estate records of private customers, held with an expectation of confidentiality and detailing personal private matters. These records often detail deeply personal information about the lives of ordinary New Zealanders and their families, and it not appropriate for public disclosure or access. Public Trust's view is that this customer information should never be made publicly available, and welcome further engagement with Archives about the most appropriate treatment for these document categories, and in particular, whether they truly are 'public records'. This will be material to Public Trust's treatment of records moving forward and may impact a number of findings in this audit. For example, the audit makes findings in respect to our storage of customer files. However, if these are not 'public records' then the treatment and associated findings may be different. Public Trust welcomes engagement with Archives on this issue prior to finalisation of the report, as the impact could potentially be significant. If such engagement is not possible prior to finalisation of the report, we note it may be beneficial to caveat some of the findings subject to this consideration occurring.

KPMG

© 2022 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

kpmg.com/nz

© **2022** KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

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

13 May 2022

Glenys Talivai
Chief Executive
Public Trust
Glenys.talivai@publictrust.co.nz

Tēnā koe Glenys

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the Public Trust 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 Public Trust is currently operating mostly at the Beginning maturity level. It is encouraging to note that an external IM review was conducted in 2021 and improvements are now being implemented as outlined in the audit report in section 6: *Summary of feedback.* Ongoing commitment to the recommendations of the review and this audit will help the Public Trust to improve its IM maturity from the currently consistently low levels. Improvements in 2022 are stated to include recruitment to an IM position as currently there is no specialist IM staffing.

In section 6 of the audit report, the Public Trust asks about the public record status of records received from clients (which is most of your information). The PRA definition of a public record is broad and any information that you receive from your clients would be deemed a public record. However, management of a public record does not necessarily mean that it is released to the wider public or transferred to Archives. This would be decided when establishing a disposal authority and associated access authority. This process determines how the information should be disposed of through transfer or destruction, and what access conditions should be set for retained information. The process would also serve to double check the PRA status of client records.

Prioritised recommendations

The audit report lists 26 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 six 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 Brad St Clair, General Manager, Legal and Governance brad.stclair@publictrust.co.nz (Executive Sponsor)

APPENDIX

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
Governance	1: IM strategy	*Complete the work programme to develop the information strategy. The information management strategy should be approved by senior management, communicated to all staff and contractors, and reviewed on a periodic basis to ensure it continues to align with PT's business activity.*	Commitment to establishing a strategy is given in section 6 following the external IM review. Involvement and approval by the newly established IM Governance Team will be essential to uplift IM across the organisation.
Governance	3: Governance arrangements and Executive Sponsor	*Design reporting that provides useful and actionable information for the Executive Sponsor. Establish regular reporting once strategies and polices are established at PT.*	A concerted effort across the organisation supported by the Executive Sponsor will be needed to improve IM practice. Regular reporting will ensure that the Executive Sponsor can monitor improvement activity with the support of the IM Governance Team.
Capability	8: Capacity and capability	*Assess information management capability and capacity requirements against business needs and consider training opportunities for information management champions to support the Executive Sponsor and the information management role once appointed.*	Public Trust's proposed model of business champions supported and lead by staff with IM experience should increase knowledge throughout the organisation. Section 6 of the audit report affirms Public Trust's intention to increase capability and uplift maturity.
Creation	10: Creation and capture of information	Identify and address information usability, reliability and trust issues.	Limiting the environments where information can be saved is the beginning of control, but the issues need to be well understood before IM solutions can be applied to improve information usability, reliability and trust issues.

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
Creation	High-value/high-risk information	Create an information asset register that identifies the information that is high-value or high-risk to PT and develop a plan for the long-term management of this information across the organisation.	This can be done in conjunction with development of the organisation-specific disposal authority and will assist in prioritisation of activity.
Disposal	20: Current organisation-specific disposal authorities	*Prioritise the development of an organisation-specific disposal authority. PT have never had an organisation-specific disposal authority.*	For an organisation creating and managing information important to New Zealander's lives this is a priority so that Public Trust understand their priorities in managing information and have an agreed disposal regime to work within. This will provide assurance to the organisation on the appropriate management of personal information.