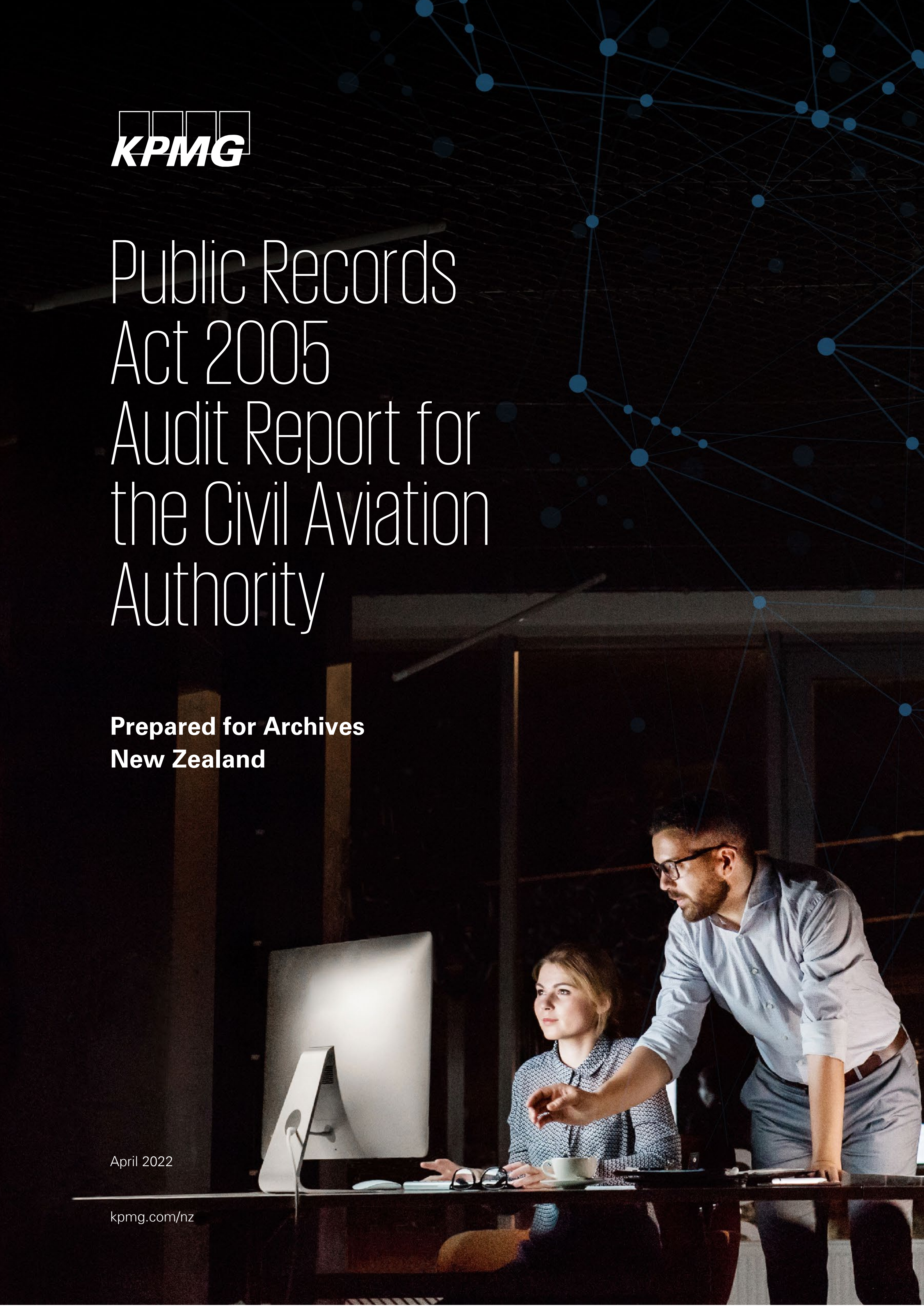

# Public Records Act 2005 Audit Report for the Civil Aviation Authority

**Prepared for Archives New Zealand**

April 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 Civil Aviation 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 Civil Aviation 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 Civil Aviation 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 Civil Aviation Authority (CAA) is the Crown entity responsible for aviation safety and security regulation, and the security service function which is delivered by the Aviation Security Service (Avsec).

The CAA creates high value public records including documents relating to aeronautical studies, medical general directions, certifications, accident investigations, airspace navigation, surveillance, aviation hazards, standards and codes of practice, international services, and inter agency agreements and environmental sustainability records. Avsec creates high value information including documentation on threats and issues facing aviation security, intelligence, Pacific Islands funding and visit reports.

The CAA has an Enterprise Content Management System (ECM) which contains high risk, high value information.

The CAA has approximately 1500 full time equivalent staff members, including the Information and Technology team that contains the Chief Information Officer and Information Management Staff such as  the Information Architect and Information Technology staff. Most records are maintained electronically, with physical records stored offsite with a third party provider.

The CAA'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** | **3** |
| **Progressing** | **13** |
| **Managing** | **3** |
| **Maturing** | **1** |
| **Optimising** | **0** |

# 2. Introduction

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

The CAA'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 Civil Aviation Authority and Avsec, including both physical and digital information.

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

The audit reviewed the CAA'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 CAA 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 CAA does not currently have a specific information management strategy to provide strategic direction and support for information management activities. There is limited content about information management in the CAA's Digital Services Strategy that was signed off in February 2022. The CAA is currently planning to develop a specific information management strategy that will align with existing strategies and support the strategic direction of the CAA.

Senior management supports the strategic direction of information management by adopting effective records management systems and advocating for their use across the CAA.

*Recommendations*

Develop an information management strategy following Archives New Zealand's guidance. The strategy should be communicated to all staff and contractors and reviewed on a periodic basis to ensure it aligns with the CAA's business activity.

### TOPIC 2 – IM policy and processes

**Progressing**

*Summary of findings*

The CAA approved an Information and Records Management Policy (Policy) in 2018 that outlines the organisation's requirements under the PRA. Information management staff are currently reviewing and updating it for the first time since it was approved to ensure it includes principles that align with legislation and the Archives New Zealand standard and requirements. The Policy documents all roles and responsibilities and is linked to other policies, including the Controlled Documents Policy, which is reviewed every three years. Policy requirements are actively built into information systems, such as a pop-up recommendation to save documents to the ECM every time a document is saved.

Details on information management processes are available on the intranet for all staff. These processes are covered through the information management training staff and contractors receive during their induction. Extra support is provided by information management staff upon request. All staff are actively encouraged to meet their information management responsibilities. However, some contractors may not receive the same encouragement as permanent staff. Staff interviewed noted that breaches of the Policy and processes were raised and addressed appropriately through escalation to a manager, the Chief Information Officer or the Legal team depending on the breach.

*Recommendations*

Update the Policy to ensure it is consistent with the information management strategy and aligns with legislation and the Archives standard and include a regular review date.

## TOPIC 3 – Governance arrangements and Executive Sponsor — Beginning

*Summary of findings*

The CAA does not have an information management governance group as management do not believe that a specific forum for information management is currently required. Any information management initiatives are raised through general management processes such as the Investment Governance Committee.

The Executive Sponsor had only been in the role for three weeks at the time of the audit. They indicated an awareness of the role, responsibilities and the importance of information management but had not yet had the time to fully act in this role. There is no regular reporting of information management activities to the current, or previous, Executive Sponsor as issues are only escalated as required.

*Recommendations*

Ensure that the governance committee overseeing information management has this included in their Terms of Reference and are accountable for it.

Design regular reporting that provides useful and actionable information to the Executive Sponsor to monitor performance and address potential risks.

## TOPIC 4 – IM integration into business processes — Progressing

*Summary of findings*

Responsibility for information management is consistently assigned to business owners in accordance with the Policy. However, the staff members interviewed noted some individuals may not be aware that they are business owners, as some names and role titles in the Policy need updating. The CAA intends to review this when the Policy is updated to ensure business owners are aware of their information management responsibilities.

Information management is integrated into most business processes and activities. Information management staff are involved in all large technology projects to ensure information management requirements are met. Information management is central to the CAA's current transition from its data centre to the cloud, and information management staff have been engaged throughout the process.

*Recommendations*

Review the policy and update the list of business owners to ensure they are up to date. The details of business owners should be updated on a regular basis to ensure roles are accurate.

Communicate these roles and responsibilities to all relevant business owners regularly.

## TOPIC 5 – Outsourced functions and collaborative arrangements — Beginning

*Summary of findings*

Collaborative agreements and outsourced functions with external agencies include requirements for storing and sharing information. For example, the CAA has Memoranda of Understanding with related agencies which detail the CAA's requirements for transferring sensitive information. Secure records management is central to these agreements.

Information management roles and responsibilities are identified in some third-party contracts, however this is inconsistent. Typically, the CAA relies on its Policy to outline roles and responsibilities. However, the Policy is not current, and not all third-party contractors are provided with this Policy. The CAA relies on inbuilt records management procedures, such as saving all documents to their ECM, to ensure compliance with the PRA. However, this may result in some external parties having limited awareness of the public records status of the records they hold.

Monitoring contracted parties is currently limited. However, a Supplier Management Governance Framework is being developed by the CAA to better monitor contracted parties.

*Recommendations*

Provide all third-party contractors with the Policy that outlines their roles and responsibilities at the induction and ensure all parties are aware of the public records status of the records they hold.

Review all existing outsourced contracts and collaborative agreements that may produce or contain high-risk or high-value information and identify what information management requirements need to be addressed.

## TOPIC 6 – Te Tiriti o Waitangi

**Beginning**

*Summary of findings*

The CAA has not identified any information that they hold that is of importance to Māori, nor have they reviewed the information management implications of Te Tiriti o Waitangi in relation to the information that the CAA creates. However, staff indicated that there have been discussions around building their knowledge through the Māori Capability Programme that the Learning and Development team is operating.

*Recommendations*

Undertake an exercise to identify and assess whether the information held by the CAA is of importance to Māori. The outcome of this exercise will inform the CAA of 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

**Progressing**

*Summary of findings*

Information management staff conduct some monitoring of the information management Policy and processes. For example, information management staff remove old users from the ECM, follow-up with users who have been inactive and view access against permissions required for staff to complete their roles. Additionally, information management staff work closely with the Risk and Assurance Team and use ComplyWith regularly to monitor their compliance with PRA requirements and other legislative standards. Where opportunities for improvement are identified, the CAA use a planner board to track how these can be implemented. However, corrective actions to address compliance issues are inconsistent and depend on the situation.

Overall, self-monitoring is limited, and information management staff have indicated they would like to implement a monitoring assurance programme to ensure more regular and comprehensive monitoring.

*Recommendations*

Develop a monitoring plan around identified areas of information management that require regular monitoring and regularly report the monitoring outcome to the Executive Sponsor.

## Capability

Information underpins everything our public offices do and impacts all functions and all staff within the public office. Effective management of information requires a breadth of experience and expertise for IM practitioners. Information is a core asset and all staff need to understand how managing information as an asset will make a difference to business outcomes.

### TOPIC 8 – Capacity and capability

**Managing**

*Summary of findings*

The CAA has appropriate information management staff capability and capacity to support staff information management. Recruitment is completed in line with current and future business needs. For example, the Deputy Chief Executive is currently reviewing whether the Information Technology (IT) team is well structured to support future business direction and needs.

Information management staff can choose the professional development opportunities they want to pursue, and staff members interviewed indicated that they receive sufficient training for their roles.

While job descriptions are not scheduled for regular review and update, they are updated as required, such as when hiring new staff or when a job description is identified as being out of date.

*Recommendations*

Regularly and proactively schedule the review of job descriptions for internal information management staff to ensure they meet current and future business needs.

### TOPIC 9 – IM roles and responsibilities

**Progressing**

*Summary of findings*

Information management roles and responsibilities are outlined in the job descriptions for information management staff and some IT roles. Information management responsibilities are also included in the Code of Conduct and to a limited extent across most CAA staff's performance plans. Information management staff supported incorporating information management roles and responsibilities into all job descriptions and performance plans.

Information management responsibilities are communicated to all staff through induction. However, staff interviewed noted that some short-term contractors may not have attended an induction if they were only briefly in the role and will therefore be lacking in information management knowledge.

Information management staff are proactive in identifying gaps in information management training, by talking with staff and observing common issues. Additional training is provided where required. The staff members interviewed felt information management staff were very thorough and supportive with their training. The CAA has recently launched a new Learning Management System and plans to develop annual information management refresher training through this platform to maintain standards across all staff.

*Recommendations*

Incorporate information management roles and responsibilities into all job descriptions and performance plans.

Ensure all contractors complete an induction.

## 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*

Most staff and contractors are aware of the legal obligation to create full and accurate records. This understanding is built through new starter onboarding and informal communications from information management staff.

Information is managed in reliable and corporate approved environments, and the use of uncontrolled environments is actively discouraged. Information management staff regularly communicate the importance of using corporate systems, particularly when working from home, including the use of the ECM. Staff cannot access corporate systems via personal laptops.

Metadata is routinely created to support the usability, reliability and trustworthiness of information. Metadata is automatically captured in the ECM and reduces the need for users to manually enter or create metadata, creating consistency.

Information management staff identified that some monitoring and reporting is completed to determine if information is usable, reliable and trustworthy. This monitoring is inconsistent, without a structured approach to identifying and addressing issues.

*Recommendations*

Develop a structured approach to monitoring and addressing information usability, reliability and trust issues across all corporate systems.

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

**Managing**

*Summary of findings*

The CAA has an information asset register that formally records high-value and high-risk information assets. However, there is no documented process to ensure the asset register is routinely updated.

Risks to high-value and high-risk information assets are identified as part of the risk assessment completed prior to the CAA adopting any new system that will hold public records. They also conduct risk assessments by enquiring with business units to determine the impact of inappropriate access to information and use access controls to mitigate this risk.

*Recommendations*

Create a process to ensure the information asset register is maintained and kept current.

## 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

**Maturing**

*Summary of findings*

Information management staff are fully involved in the design, configuration and implementation of projects involving new and upgraded business systems. The CAA has a robust change advisory process that requires all projects involving new and upgraded business systems to involve information management staff and at least two managers. This ensures information management requirements are implemented across all new and upgraded business systems, for example, when moving to their current ECM.

Information management staff are routinely involved in decommissioning business systems to ensure information management requirements are met. An example of this was the information management staff involvement in decommissioning the former intranet that was used as an information management system.

Information management requirements are being addressed in the current migration from the CAA's data centre to the cloud. They were also central to the design of the ECM. This included the use of metadata to tag information with the appropriate retention period, ensuring information of long-term value is retained appropriately.

Risks relating to business systems that do not meet information management requirements are identified and addressed. Information management staff undertake a comprehensive process to determine a system's ability to meet information management requirements prior to deciding whether to implement it.

*Recommendations*

Integrate and embed the organisation-specific disposal authority requirements into the ECM once the CAA organisation specific disposal authority is approved.

### TOPIC 13 – Integrity of information

**Progressing**

*Summary of findings*

Different business units across the CAA use varying information management practices such as file structure and the use of naming conventions. Within each business unit, these practices are routinely followed by staff and contractors to ensure that information held by the CAA is reliable and trustworthy. As a result, the staff interviewed were confident that the information they find and retrieve is comprehensive and complete.

Staff interviewed identified that information could be difficult to find and retrieve. Staff stated that it could be time-consuming and difficult to find information in the ECM due to different business units using different file structures and conventions. However, after some searching or support from information management staff, information can usually be found. Staff interviewed also identified instances of information being saved in the wrong locations.

Information management controls are in place to ensure information is reliable and trustworthy. Information management staff manage access control, version control and metadata through the ECM. However, this is done on an inconsistent basis.

*Recommendations*

Review the file structures of all business units to ensure they meet the needs of the business, including the ease of finding information.

Implement refresher training for staff covering how and where to save information to ensure information is saved in the correct place.

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

*Summary of findings*

Information management staff are routinely involved in business and system change planning. A recent example is the current migration from the CAA's data centre to the cloud. Information management staff are involved in ensuring this continues to align with the PRA.

Preservation needs for physical information are addressed as all high-value physical information held by the CAA is stored and managed offsite with a third-party provider.

Risks to the ongoing accessibility of physical information have been identified and mitigated. There are strategies to manage and maintain physical information during some business and system changes. In the recent move from their offices, CAA created a list and location register of all physical information so it can be easily accessed from their offsite storage provider. They also digitised all critical physical information.

The risks to the ongoing accessibility of digital information have been identified, and some have been mitigated. For example, the CAA recognises the risks of technology obsolescence and avoids using systems that are not well supported to mitigate this. Where they have to use these systems, they ensure a backup of all information is kept in case of the risk of obsolescence. However, other risks are not yet mitigated. For example, some digital information is stored in formats that may not be accessible in the future. The CAA is investigating ways to ensure this information can be accessed long term.

There are strategies in place to manage and maintain digital information during some business and system changes. The CAA has an information asset register in which all critical information is identified and can use this to ensure information is maintained. Access control is used for all users, and this is monitored to ensure it remains appropriate.

*Recommendations*

Continue to investigate ways to ensure all high-value digital and information can be maintained and accessed into the future.

Establish a periodic review of ongoing accessibility risks for digital information.

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

*Summary of findings*

The CAA has a Business Continuity Plan (BCP) in place that was last reviewed and updated in March 2021. The BCP describes the ECM as a critical system and outlines how to access servers and what to do in the event of a power outage to enable access to digital information. It also covers the key activities for each business unit and the timeframes in which these must be achieved to allow them to continue business as usual. However, the information critical to these activities is not explicitly identified in the plan.

The BCP also includes the restoration of physical information, including how to retrieve information from the CAA's offsite storage provider, where all critical business information is stored.

The CAA completes some testing over some system's backup and restore processes. The CAA adopted a new solution three years ago that allows them to simulate a backup without doing a restore. At the time of this audit, the most recent successful restore was completed two weeks ago.

The CAA undertakes incremental backups of digital information every night and does a complete backup at the end of each week. These backups are saved into the data centre and on a yearly basis are saved onto tapes and provided to the CAA's offsite storage provider for long term storage.

*Recommendations*

Ensure critical information identified in the Information Asset Register is included in the Business Continuity Plan.

Review the retention process for backup tapes.

## Storage

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

### TOPIC 16 – Appropriate storage arrangements

**Progressing**

*Summary of findings*

The CAA has some protection and security controls in place for physical information. The majority of physical information is stored offsite with an offsite storage provider.

Digital information is secured from unauthorised access by restrictions set by Information and Technology staff. Information and Technology staff also run danger word searches, where they identify if problematic words are being searched for. They use this to determine if information can be accessed inappropriately by staff. Backups of information are held for the appropriate period of time to avoid information being accidentally deleted. This information is currently held in a data centre, and the CAA is currently migrating from this to cloud storage.

The CAA undertake regular monitoring and receive alerts regarding protection and security processes. Alerts are reported to the Executive Sponsor on an as-needed basis.

*Recommendations*

Establish a periodic review of the digital storage environment and the protection and security measures in place, to ensure controls remain appropriate and fit for purpose. Report findings to the Executive Sponsor.

## 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 CAA uses metadata and file structures to ensure reliable management and discovery of information. File structures and naming conventions are used by each business unit and were developed with the information management staff's input and guidance.

Information management staff have to manually identify whether information is open or restricted access. However, metadata such as the unique identifier, name of the document, date created, business activity documented, creator, actions carried out, identification of the person carrying out the action and the date these actions were carried out is automatically applied wherever possible.

Access rights to ECM documents are set up by the information management staff, and any access controls issues are addressed promptly. The ECM runs regular reporting on staff access permissions. Information management staff document instances of significant changes, for example, adding the legal department to certain folders.

Staff interviewed reported having the proper access to all the information they need to perform their job for the most part. If they do not have appropriate access, this is quickly rectified. Only authorised staff can access sensitive files, and audit trails show who has accessed or modified documents.

Staff interviewed were confident in using the systems due to their induction training. However, staff did note that finding information could be complex due to the nature of the work and the structure of the systems used. Further training or support on this is available on request.

*Recommendations*

Ensure that Archives New Zealand's minimum metadata requirements are met for all relevant business systems.

## Disposal

Disposal activity must be authorised by the Chief Archivist under the Public Records Act. Public offices should have their own specific disposal authority as well as actively use the General Disposal Authorities for disposal of general or more ephemeral information. Disposal should be carried out routinely. Information of archival value, both physical and digital, should be regularly transferred to Archives New Zealand (or have a deferral of transfer) and be determined as either "open access" or "restricted access".

## TOPIC 20 – Current organisation-specific disposal authorities

**Progressing**

*Summary of findings*

The CAA has one disposal authority that covers all CAA's information formats and business functions. This expired in June 2021 and was extended in December 2021 until June 2023.

A second disposal authority covers all information formats and business functions of Avsec. Avsec's disposal authority was approved in 2013 and expires in 2023.

Staff and contractors understand that disposal is handled by information management staff. The Information Architect, who is part of the wider Information and Technology team, plans to review the recently expired disposal authority to ensure it is still appropriate for all information that the CAA holds. However, there is no formal, regular review in place.

*Recommendations*

Establish a formal review cycle and ensure changes identified during the review are incorporated into the organisation-specific disposal authority.

## TOPIC 21 – Implementation of disposal decisions

**Progressing**

*Summary of findings*

A delegation system is in place for disposal actions to be performed. The Information Architect identifies information that is potentially ready for disposal through the General Disposal Authority or Avsec's disposal authority and shares this with the relevant business owner for review. Once approved, the Chief Information Officer conducts a review to ensure it can be disposed of. The Information Architect then actions the disposal.

The destruction of most digital information is secure, complete and irreversible. The one area of concern identified was backup tapes of servers, and information staff were not confident they had oversight across this information. The destruction of physical information is secure, complete and irreversible. Information management staff noted information has never been disposed of under the CAA disposal authority as all this information is still required for business use.

All information stored in the ECM is marked with a disposal action. The ECM has the functionality to action these disposals but the CAA has not yet done this.

*Recommendations*

When the disposal authority has been approved apply the retention and disposal actions to the ECM.

## TOPIC 22 – Transfer to Archives New Zealand

**Progressing**

*Summary of findings*

In 2016 the CAA was part of a pilot to transfer digital information of archival value to Archives New Zealand. CAA has identified all information over 25 years that is of archival value, but still requires this for business activities so has not transferred any to Archives. The CAA had a deferral of transfer agreement, however this expired in 2021.

*Recommendations*

Update the deferral of transfer agreement.

# 6. Summary of feedback

The Authority's resources have been severely limited by the COVID-19 pandemic. Our third-party revenue (i.e. the funds we receive through fees, levies was 55% lower than in 2019/20 (before the pandemic). To address this shortfall, we have had to cut resourcing and funding in our non-core regulatory functions – such as information management – and we have relied heavily on Crown-funding through the COVID-19 liquidity facility, which was established to support the Authority to remain solvent.

The Authority continues to remain insolvent and is reliant on letters of support from the Minister of Finance and the Crown liquidity facility to remain solvent and a going concern for FY23 and FY24.

In principle we accept the summaries of findings and recommended actions and these will be incorporated into action plans as funding and resourcing becomes available but this is unlikely this will occur before FY25 (or beyond) given the liquidity challenges (described **above**) so the Authority cannot make any representations or warranties when the findings and recommended actions will be addressed.

Any direct support from Te Rua Mahara o te Kawanatanga I Archives New Zealand to support the Authority to address the findings and recommended actions would be much appreciated as Authority is committed to remediating these actions but resourcing and funding is not available in the short and medium term.

**kpmg.com/nz**

Te Rua Mahara o te Kāwanatanga
archives
NEW ZEALAND

17 August 2022

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

Keith Manch
Chief Executive
Civil Aviation Authority of New Zealand
keith.manch@caa.govt.nz

Tēnā koe Keith

**Public Records Act 2005 Audit Recommendations**

This letter contains my recommendations related to the recent independent audit of the Civil Aviation Authority of New Zealand (the CAA) 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 CAA is mostly operating at the ‘Progressing’ level with some topics at higher levels. It is well placed with an ECM, current disposal authority and IM staffing to move to ‘Managing’ level with support from the senior management level of the organisation. The current challenging operating environment can be considered when developing a strategy and most recommendations have minimal financial impact.

### *Prioritised recommendations*

The audit report lists 27 recommendations to improve your organisation’s IM maturity.

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

### *What will happen next*

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

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

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

Thank you again for your support with the audit. We would greatly appreciate further feedback on the audit process and the value it provides to organisations, and we will contact your Executive Sponsor shortly in relation to this.

Nāku noa, nā

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

Cc Mark Davis, DCE Corporate Services (Executive Sponsor), mark.davis@caa.govt.nz

## 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. The strategy should e communicated to all staff and contractors and reviewed on a periodic basis to ensure it aligns with the CAA's business activity.* | CAA is currently planning to develop a strategy. A strategy is necessary to determine the IM direction within CAA's current financial situation. |
| **Governance** | 2: M policy and processes | *Update the Policy to ensure it is consistent with the information management strategy and aligns with legislation and the Archives standard and include a regular review date.* | It is important that the Policy is kept up to date and communicated to all staff to ensure staff are aware of their current roles and responsibilities (see Topic 4: IM integration into business processes) |
| **Governance** | 3: Governance arrangements and Executive Sponsor | *Ensure that the governance committee overseeing information management has this included in their Terms of Reference and are accountable for it.* | A committee that has IM as part of its ToR is useful support for the Executive Sponsor in implementing a strategy and overviewing IM in the organisation. |
| **Governance** | 5: Outsourced functions and collaborative arrangements | *Review all existing outsourced contracts and collaborative agreements that may produce or contain high-risk or high-value information and identify what information management requirements need to be addressed.* | Existing and new contracts should include roles and requirements for managing any public records involved. These requirements should be monitored to ensure that the records are managed appropriately. |
| **Self-monitoring** | 7: Self-monitoring | *Develop a monitoring plan around identified areas of information management that require regular monitoring and regularly report the monitoring outcome to the Executive Sponsor.* | This will assist the Executive Sponsor in oversight of IM across the organisation and in communication with the governance group. This also relates to Topic 10: *Creation and capture of information* |

| Category | Topic Number | Auditor's Recommendation | Archives New Zealand's Comments |
|---|---|---|---|
| **Management** | 13: Integrity of information | *Review the file structures of all business units to ensure they meet the needs of the business, including the ease of finding information.* | This will increase efficiency and assure the CAA that information is able to be found and IM systems are reliable and trustworthy. |
| **Disposal** | 20: Current organisation-specific disposal authorities | *Establish a formal review cycle and ensure changes identified during the review are incorporated into the organisation-specific disposal authority.* | As both disposal authorities will expire in 2023 it is important that development of new disposal authorities is started. This will ensure that the process is completed in time and the CAA maintains disposal coverage. |
| **Disposal** | 22: Transfer to Archives New Zealand | *Update the deferral of transfer agreement.* | Ensure that the agreement is still fit for purpose and either update or request renewal from Archives New Zealand. |