



# Public Records Act 2005 Audit Report for Fire and Emergency New Zealand

**Prepared for Archives  
New Zealand**

June 2022

[kpmg.com/nz](https://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 Fire and Emergency New Zealand. 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 Fire and Emergency New Zealand 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 Fire and Emergency New Zealand'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

<b>1. Executive summary</b>	<b>1</b>
<b>2. Introduction</b>	<b>2</b>
<b>3. This audit</b>	<b>2</b>
<b>4. Maturity Assessment</b>	<b>3</b>
<b>5. Audit findings by category and topic</b>	<b>4</b>
Governance	4
Self monitoring	7
Capability	7
Creation	8
Management	9
Storage	11
Access	11
Disposal	12
<b>6. Summary of feedback</b>	<b>15</b>



# 1. Executive summary

Fire and Emergency New Zealand (FENZ) exists to carry out a range of functions, such as ensuring the safety of persons in the event of fire, medical emergency, and natural hazards. FENZ was formed in 2017 after merging 40 separate entities into a single organisation, therefore inheriting records from its predecessor organisations. FENZ has approximately 3000 staff and more than 10,000 volunteers throughout New Zealand.

FENZ uses shared drives as a primary store for digital information. Many additional systems are used to create and manage information related to specific functions such as finance, station management, and asset management. FENZ has a large quantity of physical information, the majority of which is stored offsite with a commercial storage facility.

At the time of this audit, one skilled and dedicated Senior Advisor Records Management had been in the role for eight weeks. FENZ receives additional support from an external information management consultant. There was no governance group responsible for information management.

The information management maturity of FENZ is summarised below. Further detail on each of the maturity assessments can be found in sections 4 and 5 of this report.

<b>Beginning</b>	<b>11</b>
<b>Progressing</b>	<b>9</b>
<b>Managing</b>	<b>0</b>
<b>Maturing</b>	<b>0</b>
<b>Optimising</b>	<b>0</b>



## 2. Introduction

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

FENZ'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 FENZ including both physical and digital information.

The audit involved reviews of selected documentation and interviews with selected staff, including the Executive Sponsors, records management staff, the information and communications technology (ICT) team, and a sample of other staff members from various areas of FENZ. Note that one of the Executive Sponsors has delegated responsibility for managing the Public Office's recordkeeping obligations under the Public Records Act including development and maintenance of policies, manuals, training, disaster recover, storage and records disposal, and is the senior responsible officer for the audit.

The audit reviewed FENZ'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. FENZ 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
<b>Governance</b>							
	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	●				
<b>Self-monitoring</b>							
	7	Self-monitoring		●			
<b>Capability</b>							
	8	Capacity and capability		●			
	9	IM roles and responsibilities		●			
<b>Creation</b>							
	10	Creation and capture of information		●			
	11	High-value / high-risk information	●				
<b>Management</b>							
	12	IM requirements built into technology systems	●				
	13	Integrity of information		●			
	14	Information maintenance and accessibility	●				
	15	Business continuity and recovery	●				
<b>Storage</b>							
	16	Appropriate storage arrangements		●			
<b>Access</b>							
	18	Information access, use and sharing	●				
<b>Disposal</b>							
	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*

FENZ has an Enterprise Information Management Strategy (EIMS) dated June 2020. The EIMS contains a three-year roadmap identifying actions to uplift FENZ's information management competence and maturity. However, because there is no governance group in place for information management (see Topic 3 – *Governance arrangements and Executive Sponsor*), there is no mechanism in place to promote and monitor progress against activities contained in this roadmap.

Records management staff noted during interviews that the EIMS was approved by the appropriate governance group (which was recently retired), but its status as a finalised document remains unclear. For example, there are no signatures on the document or sign-off dates, and the current version is titled "final draft".

The strategy has not been effectively communicated to staff. Most staff interviewed were not aware of the existence of the EIMS or had not yet seen it. Some staff who were aware of the strategy commented that it does not seem to inform strategic decision making, and work is required to translate the EIMS into actionable items. For an information management strategy to be successful in steering decision making, it is important that it is endorsed and promoted by senior leadership.

#### *Recommendations*

Finalise the EIMS and ensure it is signed-off, endorsed and promoted by appropriate leadership members.

### TOPIC 2 – IM policy and processes

Progressing

#### *Summary of findings*

FENZ has a Records Management Policy, covering information management principles and responsibilities. The policy references the Archives New Zealand Electronic Recordkeeping Metadata Standard, Public Records Act and other legislation. The policy was last updated in April 2019 but has a review period of two years. It is therefore out of date. The Senior Advisor Records Management noted there is a plan to rewrite this policy so that it specifically aligns with the Archives New Zealand Information and Records Management Standard. This is consistent with the EIMS roadmap, which contains an action to "review information-related policies".

There is guidance available on the intranet for managing information; this was last reviewed in November 2020. The guidance covers topics such as what information must be kept, where to save it, naming and version control, and guidance on what information can be destroyed. But many staff reported that they had not viewed this guidance material. Some staff interviewed said they receive business unit specific guidance through on-the-job training. Not all business units have documented processes for information management.

Staff interviewed were aware of their information management responsibilities. Some staff reported that information management responsibilities are included in their job description due to the nature of the work they do. In addition, many staff members noted that responsibilities were communicated to them by their manager. There was also some awareness of legislative requirements, such as the need to retain public records and the requirements under the Official Information Act.

### ***Recommendations***

Update the Records Management Policy and ensure it aligns with the organisation's information management strategy and the Archives New Zealand Information and Records Management Standard.

Develop best practice information management guidance for FENZ, including business unit specific information management procedures as required.

## **TOPIC 3 – Governance arrangements and Executive Sponsor**

**Beginning**

### ***Summary of findings***

Two Deputy Chief Executive level staff fulfil the Executive Sponsor role. However, primary responsibility rests with the Deputy Chief Executive Organisational Strategy and Capability Development.

There is no governance group currently overseeing information management at FENZ. There was previously a governance group in place, the Intelligence, Information and Innovation Panel ("Triple I panel"), which received quarterly information management reporting. However, this governance group was retired in December 2021 as part of a wider Executive Leadership Team sub-panels governance group review process. There are ongoing discussions to transfer the information management governance function to the Security Reference Group.

At the time of the audit, reporting is provided to the Executive Sponsors if requested. But this is not a regular activity. Given the shared responsibilities in this area, it is not always clear to whom information should be directed to for decision making.

### ***Recommendations***

Transfer information management governance to an appropriate governance group and update the relevant Terms of Reference to reflect this. Ensure there are clear areas of responsibility for the Executive Sponsor.

Establish regular information management reporting to the Executive Sponsor and governance body.

## **TOPIC 4 – IM integration into business processes**

**Beginning**

### ***Summary of findings***

Discussions with staff highlighted that there is not always a clear sense of who has ownership of information management within different areas of the organisation. For example, business owner responsibilities are not documented.

Some business units have good guidance available for managing information that has been created by staff. Requirements for ensuring records are accessible and reliable are integrated into how these units carry out their business-as-usual activities. For example, the team responsible for claims management have process maps and detailed processes which show where information should be stored within the system as they carry out their work. Documents within this system are stored in dedicated locations to provide confidence in the completeness of records. Staff indicated that for project-based teams, there is no standard for what is required for information management. This leads to different outcomes between projects for integrating information management into their workflow. We were, however, provided with a roadmap that outlines standardised information management requirements for projects within the Investments Portfolio.

There is no clear process for managing information when staff leave the organisation. It relies on the respective manager to organise the transfer of any information not yet stored on drives accessible by other staff. Records



management staff suspect that this process gap may have led to information being lost or deleted when staff, contractors or volunteers have left the organisation.

### ***Recommendations***

Document information management responsibilities for business owners at FENZ.

Develop a standardised process for the management of information when staff and contractors leave FENZ.

---

## **TOPIC 5 – Outsourced functions and collaborative arrangements**

**Beginning**

### ***Summary of findings***

Requirements for managing information are detailed in some but not all contracts where there are outsourced functions or collaborative arrangements. Of the contracts sampled, one contained a clause relating to records management responsibilities, including a reference to the Public Records Act. This contract specified that all data, documents, and other information received or created in relation to the service are owned by FENZ. However, records management staff noted that this is not the case for all contracts and that there are not always clear clauses on ownership of the information or details of an exit strategy.

There was no evidence of monitoring over contracted parties to ensure information management requirements were met. However, one contract did specify the ability for FENZ to audit the service provider to monitor compliance with the terms of the contract.

### ***Recommendations***

Develop standardised information management requirements that can be used when creating contracts for outsourced functions and collaborative agreements where public records are created and managed.

Conduct monitoring of contracted parties to ensure information management requirements, as specified in the relevant contracts, are being met.

---

## **TOPIC 6 – Te Tiriti o Waitangi**

**Beginning**

### ***Summary of findings***

The National Strategy 2019 – 2045 for FENZ describes a commitment to working with Māori as tangata whenua. However, this has not yet been operationalised into information management activities. FENZ has not identified information of importance to Māori and acknowledges that this will require working closely with different iwi to ensure it is done in a meaningful way. Some thought has been given to this, such as the need to identify relevant iwi or hapū for property records.

### ***Recommendations***

Undertake an exercise in consultation with Māori to identify information held by FENZ, which is of importance to Māori. The outcome of this exercise should inform FENZ of what actions are necessary to ensure any relevant information is accessible and managed with appropriate care in the future.

## 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*

FENZ performs some compliance monitoring of their legislative requirements and policy. For example, in November 2021, FENZ brought in external expertise to carry out annual compliance monitoring, which included surveying managers and key staff on compliance with the Public Records Act. In addition, FENZ has previously contracted an external service provider to complete an information management audit. This was conducted in June 2020 and pertained to both electronic files and physical files. These audits demonstrate initiative in trying to understand and improve the way that FENZ manages its information. However, monitoring activities are irregular and corrective actions to address non-compliance are inconsistent.

#### *Recommendations*

Design and agree regular information management monitoring procedures and report findings to the Executive Sponsor.

## Capability



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

### TOPIC 8 – Capacity and capability

Progressing

#### *Summary of findings*

There is limited capacity for FENZ to actively drive the activities that are required to improve the maturity of its information management practices. For example, records management staff do not think there are enough resources to carry out regular disposal decisions. This is because there is currently only one dedicated records management staff member. This staff member is being assisted by an external information management consultant who has provided support and expertise, including over the period when the business had no internal records expertise and as a member of the now retired Triple I Panel. Because of the limited information management capacity internally at FENZ, information management efforts have a reactive nature rather than proactively improving the way information is managed.

FENZ is at an early stage of identifying its current and future capacity requirements. FENZ was undergoing recruitment for a Records Advisor at the time of the audit.

There is a professional development fund that records management staff are encouraged to use.

### ***Recommendations***

Regularly assess information management capacity requirements against business needs and the Archives New Zealand Standard. Recruit additional records management staff as needed to develop information management maturity.

## **TOPIC 9 – IM roles and responsibilities**

**Progressing**

### ***Summary of findings***

Roles and responsibilities for information management are documented in some job descriptions. Information management does not currently play a part in performance plans. However, some staff noted there were plans for information management to be considered in performance plans in the future.

A records management training module was developed for Station Officer roles but is available for all staff on the learning management system. However, this module is not compulsory, and the number of staff completing this training is relatively low.

Training on information management is not consistently provided during inductions. A Legal Team staff member had received training on the legislative requirements of the Public Records Act, but most staff said they did not receive any information management training as part of their inductions. An induction checklist includes records management as a point to cover, but compliance with this checklist is not monitored.

### ***Recommendations***

Mandatory induction and regular refresher training should be provided to staff to clarify and communicate their roles and responsibilities to create, capture, and store information.

## **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***

There is some awareness among staff of their legal obligations to create and capture full and accurate records, as specified within the Public Records Act. Staff are particularly aware of the key information they create within their business unit and the need to ensure this is accessible. However, interviews with staff members identified incidents where they could not locate information relating to historic decisions that were made, which suggests some information was not being captured or managed appropriately.

Staff are encouraged to store information within controlled environments. This is clearly stated within the information management guidance available on the intranet. However, given the significant number of volunteers throughout New Zealand who use personal and FENZ devices for a range of activities, information and communications technology staff noted that it is difficult to control and monitor whether people are storing information in uncontrolled environments.

The quality of metadata captured is dependent on the system which is being used to create information. For example, shared drives require manual input to capture information such as the document version, creator of the document, and a relevant title. Records management staff, and staff from across the business units, are aware of the current issues within their systems that reduce the usability and reliability of information. The EIMS roadmap contains activities that should help progress maturity in this area, such as designing information architecture and organisation-wide taxonomy and developing a structured approach to data management.

### **Recommendations**

Identify information usability, reliability and trust issues across the organisation and develop an action plan to address these. This should consider information created and managed by volunteer/operational support roles throughout New Zealand.

Ensure information is managed in controlled environments to ensure its usability and reliability across the organisation.

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

**Beginning**

### **Summary of findings**

There is no formalised approach from an information management lens to identify high-value/high-risk information assets held in digital and physical systems. There is a register that identifies the systems in use by FENZ and captures some key information contained within these systems, but it is not intended to be an information asset register. The systems register identifies information critical for business operations rather than from a public records perspective.

Work is underway to identify physical information held by the commercial storage facility to understand the scope and importance of this information. Some of the records held at the commercial storage facility were obtained from the urban and rural fire services when FENZ was formed in 2017.

Without a register of high-value/high-risk information, it is not possible to have a long-term management plan in place.

### **Recommendations**

Develop an information asset register that identifies information held by FENZ that is of a high-value or high-risk nature and a plan for the long-term management of this information.

## **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 expertise is not regularly involved in the design and configuration of new or upgraded business systems. Instead, information management expertise is engaged either near a launch date or after a system has been launched.

There are no standardised information management requirements that can be used to support the implementation or upgrading of systems. We were provided with examples where the ICT function addressed information

management requirements during the design of new or upgraded systems without consulting information management expertise. Information management expertise should be involved during the design process to ensure that the appropriate considerations are made.

There is no standardised process to ensure that the minimum metadata requirements specified by Archives New Zealand are incorporated into the design and implementation of new or upgraded business systems.

### ***Recommendations***

Create standardised information management requirements for new and upgraded business systems and ensure that information management expertise is included as part of the system change process. The requirements should specify the minimum metadata that is needed to align with the Archives New Zealand Standard.

---

## **TOPIC 13 – Integrity of information**

**Progressing**

### ***Summary of findings***

Discussions with staff identified some localised information management practices across the business units. For example, staff use naming conventions, manual version control, and file structure to help manage information. However, these conventions are not consistently followed within all business units. The capability for organising and applying metadata to information depends on the systems used to create and manage that information.

While staff interviewed said information used regularly is easy to locate and access, other information can be difficult to find, particularly if a regional station holds the information. Moreover, staff said it sometimes requires multiple conversations to identify who is responsible for the information.

### ***Recommendations***

Identify the integrity issues that staff have around finding, retrieving and using information across the organisation and develop a plan to address these.

---

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

**Beginning**

### ***Summary of findings***

The EIMS provides principles and a vision for the management of information. But there were no specific strategies to help manage physical and digital information during system changes, such as a metadata continuity plan.

FENZ is beginning work to identify and categorise information held at a commercial storage facility. Technology obsolescence risks have not yet been formally identified, although ICT staff believe that the digital formats used by FENZ for unstructured data (such as PDFs) should enable usability and readability in the future.

### ***Recommendations***

Develop strategies to manage and maintain physical and digital information during business and system change projects.

Identify obsolescence risks for physical and digital information and develop a plan to address these. Establish a periodic review of these risks.

---

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

**Beginning**

### ***Summary of findings***

FENZ has a business continuity plan in place that covers the Fire and Emergency National Headquarters (NHQ), which was last reviewed in July 2019. This plan does not identify critical physical or digital information that would be

required for business continuity. It does not specify the process to salvage physical information stored at NHQ, such as physical payroll information.

FENZ keep a record of completed and scheduled disaster recovery tests for a number of the applications used by the organisation. This testing record contains a criticality classification for each application. However, the business continuity plan itself does not cover critical physical and digital information. There is no evidence of regular testing of the business continuity plan, including salvaging physical information.

### ***Recommendations***

Identify critical information and include this in business continuity plan. The business continuity plan should be tested regularly.

## **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 appropriate protection for physical information stored at the NHQ. Payroll information is stored under lock and key and there are sprinklers and fire alarms in place. Other physical information is held at a commercial storage facility, with a controlled list of staff who can authorise the disposal of information. The current process for sending information to the commercial storage provider is decentralised, and records management staff have little visibility over what is being put into storage regionally. We did not inspect any regional storage locations as part of this audit.

Several security mechanisms are in place to protect against the unauthorised access, loss and destruction of digital information. Examples include Microsoft data loss protection, malware protection, and multifactor authentication for some systems. Some testing of these controls has taken place. For example, penetration testing and security testing has been conducted for the finance system. But regular testing is not conducted across all systems.

There are limited controls for deleting information within some systems, such as shared drives. This means that staff who have access to these systems are able to delete information without requiring additional authorisation. FENZ has a backup process, which means that information can generally be restored if necessary.

### ***Recommendations***

Assess the risk to information from unauthorised deletion across FENZ systems and implement an action plan to mitigate those risks. Provide regular updates to the Executive Sponsor on progress.

## **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.

**Summary of findings**

There is a taxonomy for the national shared drive, but this is not consistently adhered to. As a result, some teams have developed their own process for categorising and structuring information within shared drives. Staff interviewed said there are differences in the structure and management of information because of the large number of systems used by FENZ staff.

Staff have not received any formalised training on metadata search techniques, but most staff felt they have an adequate understanding of the search functions within the systems that they use regularly. However, the lack of central coordination for managing information means that it can be difficult to find and access information at times.

There is good oversight of access controls for some systems used by FENZ staff. There is multifactor authentication in place and password expiration every 90 days for some systems. System owners are responsible for regularly reviewing access controls for their systems, but there is no evidence of regular reviews being carried out.

Metadata collected by FENZ does not comply with the minimum metadata requirements set by Archives New Zealand. This is partly because some systems, such as shared drives, do not have the functionality required to capture the necessary metadata.

**Recommendations**

Investigate options for replacing shared drives to enable appropriate control and management of information across FENZ, including the information created by volunteer/operational support roles.

Communicate the expectations for maintaining and structuring information to staff and contractors to ensure the findability of information. Ensure these expectations and best practices are documented and accessible by staff, contractors, and volunteers throughout New Zealand.

**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”.

**Summary of findings**

FENZ has a current and approved organisation-specific disposal authority which covers most information formats and functions. The disposal authority was approved in August 2012 and is therefore set to expire in August 2022. Records management staff noted that they had recently reached out to Archives New Zealand to apply for an extension before FENZ’s disposal authority expires. Records management staff noted there was no regular review cycle to ensure the disposal authority reflects business changes. They acknowledge that there are likely gaps in the disposal authority because new forms of information have not been identified, classified and incorporated into the disposal authority. This includes information inherited from the rural fire authorities, and information created from new outsourced functions. Records management staff expressed a desire to implement a regular review cycle in future.

### ***Recommendations***

Update the organisation-specific disposal authority to cover all formats and business functions and get it approved by Archives New Zealand.

Implement a regular review process to ensure the disposal authority remains current through business and process changes.

## **TOPIC 21 – Implementation of disposal decisions**

**Beginning**

### ***Summary of findings***

Disposal decisions have been carried out historically for physical information, but not routinely. The most recently documented physical destruction was carried out in 2012. A disposal register is maintained and captures metadata such as the authorising manager, date of disposal, and relevant class of the disposal schedule. The destruction method captured in the disposal register assures that destruction is secure, complete, and irreversible.

Digital information is kept indefinitely by default, as there is no process in place to routinely carry out disposal decisions for digital information. Records management staff believe there are insufficient resources to carry out regular disposal decisions.

Staff interviewed had an inconsistent understanding of the disposal requirements for the information they create and manage. Some staff knew that guidance was available on what could be disposed of. Others were unsure on whether guidance for disposal existed. Some staff expressed a tendency to keep everything to reduce the chance of incorrect disposal.

### ***Recommendations***

Once an up-to-date organisation-specific disposal authority has been approved (as discussed in Topic 20 – *Current organisation-specific disposal authorities*), develop a plan for regular disposal of physical and digital information.

## **TOPIC 22 – Transfer to Archives New Zealand**

**Beginning**

### ***Summary of findings***

FENZ has not carried out an assessment to identify information of archival value that is over 25 years old. Physical information has been transferred to Archives New Zealand in the past, but there has been no transfer of information since FENZ was formed in 2017. Records management staff do not believe that the metadata captured for digital information is comprehensive enough for it to be accepted by Archives New Zealand.

### ***Recommendations***

Once an up-to-date disposal authority has been approved (as discussed in Topic 20 – *Current organisation-specific disposal authorities*), FENZ should identify and assess access restrictions for any records of archival value and any that are approaching or are older than 25 years old. A deferral of transfer agreement should be obtained if necessary.





## 6. Summary of feedback

Thank you for the opportunity to review the audit report prepared by KPMG on behalf of Archives New Zealand.

We feel that the unique organisational context of Fire and Emergency regarding its information management capability and capacity has not been clearly reflected in the audit report. Fire and Emergency was created in 2017 with the amalgamation of 40 separate entities, many of which were not part of the public sector and did not have Public Records Act 2005 obligations.

Significantly, it has taken the last 5 years to settle the operational structure of Fire and Emergency into a functional whole, and within the scheme of that, we acknowledge that information and records management has not always received the focus it needs. This to some degree reflects the emergency response nature of the organisation, and the critical need to ensure that aspect of our organisation operates well.

**Withheld under principle 11, Privacy Act 2020**

Moving forward, with a united organisational structure in place and a revitalised records management team with accomplished and proficient staff, we can now start focusing on information and records management and significantly improving our maturity.

Fire and Emergency acknowledges the recommendations made, and notes that many are captured on our Records Management 5-year work plan. To support the delivery of that programme and enable us to leverage the report to make real change in the organisation we provided suggestions during the draft report stage to reframe some of the original recommendations so they would provide clear, achievable, and meaningful outcomes to help us improve our maturity.

[kpmg.com/nz](https://kpmg.com/nz)



22 September 2022

Archives New Zealand, 10 Mulgrave Street, Wellington  
Phone +64 499 5595

Websites [www.archives.govt.nz](http://www.archives.govt.nz)  
[www.dia.govt.nz](http://www.dia.govt.nz)

Kerry Gregory  
Chief Executive  
Fire and Emergency New Zealand  
[Kerry.gregory@fireandemergency.nz](mailto:Kerry.gregory@fireandemergency.nz)

Tēnā koe Kerry

### **Public Records Act 2005 Audit Recommendations**

This letter contains my recommendations related to the recent independent audit of the Fire and Emergency New Zealand (FENZ) by KPMG under section 33 of the Public Records Act 2005 (PRA). Thank you for making your staff and resources available to support the audit process.

#### ***Introduction***

Te Rua Mahara o Te Kāwanatanga Archives New Zealand (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.

#### ***Kia pono ai te rua Mahara – Enabling trusted government information***

Auckland Regional Office, 95 Richard Pearse Drive, Mangere, Auckland  
Christchurch Regional Office, 15 Harvard Avenue, Wigram, Christchurch  
Dunedin Regional Office, 556 George Street, Dunedin

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. FENZ is a significantly different organisation from its predecessors. We acknowledge the challenges that has meant for its IM, reflected in maturity ratings that have not yet reached 'Managing'.

It is heartening, however, to read the organisation's commitment to improving its IM and the confidence in the revitalised IM team from section 6: *Summary of feedback in the audit report*. Providing enough resources and IM expertise to support the team and improvement activities is key to improvement success. The 5-year work plan will assist this. In the context of that plan and the extensive change inherent in the creation of FENZ, we support your recent decision to develop a new, rather than merely updated, disposal authority.

### ***Prioritised recommendations***

The audit report lists 28 recommendations to improve your organisation's IM maturity.

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

### ***What will happen next***

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

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

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

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

Nāku noa, nā



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

Cc Russell Wood, Deputy Chief Executive (Executive Sponsor),  
[Russell.wood@fireandemergency.nz](mailto:Russell.wood@fireandemergency.nz)

## APPENDIX

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
<b>Governance</b>	1: IM strategy	<i>Finalise the EIMS and ensure it is signed-off, endorsed and promoted by appropriate leadership members.</i>	Ensure that the strategy (dated June 2020) is still fit for purpose to give the IM direction currently needed. The Records Management 5-year work plan referred to in the Audit Report section 6: <i>Summary of feedback</i> will also inform direction.
<b>Governance</b>	2: IM policy and processes	<i>Update the Records Management Policy and ensure it aligns with the organisation's information strategy and the Archives New Zealand Information and Records Management Standard.</i>	Once this is communicated it will support IM across the organisation with awareness of roles and responsibilities.
<b>Governance</b>	3: Governance arrangements and Executive Sponsor	<i>Transfer information management governance to an appropriate governance group and update the relevant Terms of Reference to reflect this. Ensure there are clear areas of responsibility for the Executive Sponsor.</i>	The governance group will have a key role with implementing the strategy and monitoring IM uplift across the organisation.
<b>Capability</b>	8: Capacity and capability	<i>Regularly assess information management capacity requirements against business needs and the archives New Zealand Standard. Recruit additional records management staff as needed to develop information management maturity.</i>	Implementation of strategic initiatives and development of a new DA will need to be resourced as well as BAU activities.
<b>Creation</b>	11. High-value/high-risk information	<i>Develop an information asset register that identifies information held by FENZ that is of a high-value or high-risk nature and a plan for the long-term management of this information.</i>	This should be done in conjunction with the work on the organisation-specific disposal authority (Topic 20) and will help FENZ by determining which information is most important to the organisation.

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
<b>Access</b>	18: Information access, use and sharing	<i>Investigate options for replacing shared drives to enable appropriate control and management of information across FENZ including the information created by volunteer/operational support roles.</i>	This activity needs to be done involving IM expertise to ensure that IM requirements for a new system are understood and able to be built in.
<b>Disposal</b>	20: Current organisation-specific disposal authorities	<i>Update the organisation-specific disposal authority to cover all formats and business functions and get it approved by Archives New Zealand.</i>	FENZ have recently advised that because the significant changes to the organisation since 2017 have resulted in gaps in coverage in the existing DA, they will start to develop a new DA rather than proceed with the update and extension as mentioned in the report. This decision is noted and supported by Archives New Zealand.