



Te Kaitiaki Take Kōwhiri  
Electoral Commission

Public Records Act 2005 Audit Report

Prepared for Te Rua Mahara o te Kāwanatanga  
Archives New Zealand

March 2023

# Table of Contents

|                                            |    |
|--------------------------------------------|----|
| 1. Disclaimers                             | 3  |
| 2. Executive Summary                       | 4  |
| 3. Introduction                            | 5  |
| 4. Information Management Maturity Summary | 6  |
| 5. Audit Findings by Category and Topic    | 7  |
| Governance                                 | 7  |
| Self-Monitoring                            | 9  |
| Capability                                 | 10 |
| Creation                                   | 11 |
| Management                                 | 13 |
| Storage                                    | 15 |
| Access                                     | 16 |
| Disposal                                   | 17 |
| 6. Summary of Feedback                     | 20 |

# 1. Disclaimers

## USE OF REPORT

This report has been prepared in accordance with the Consultancy Order Services dated 1 December 2020 and variation dated 23 September 2021. We have prepared this report solely for Te Rua Mahara o te Kāwanatanga Archives New Zealand (Archives) and Electoral Commission. It was prepared at the direction of Archives and may not include all procedures deemed necessary for the purposes of the reader. The report should be read in conjunction with the disclaimers as set out in the Statement of Responsibility section. We accept or assume no duty, responsibility, or liability to any other party in connection with the report or this engagement, including, without limitation, liability for negligence in relation to the factual findings expressed or implied in this report.

## INDEPENDENCE

Deloitte is independent of Archives in accordance with the independence requirements of the Public Records Act 2005. We also adhere to the independence requirements of the New Zealand Auditing and Assurance Standards Board's Professional and Ethical Standard 1 (Revised): Code of Ethics for Assurance Practitioners. Other than this audit programme, we have no relationship with or interests in Archives.

## STATEMENT OF RESPONSIBILITY

The procedures that we performed did not constitute an assurance engagement in accordance with New Zealand Standards for Assurance engagements, nor did it represent any form of audit under New Zealand Standards on Auditing, and consequently, no assurance conclusion or audit opinion is provided. The work was performed subject to the following limitations:

This assessment is based on observations and supporting evidence obtained during the review. This report has taken into account the views of Electoral Commission and Archives, and both have reviewed this report.

Because of the inherent limitations of any internal control structure, it is possible that errors or irregularities may occur and not be detected. The procedures were not designed to detect all weaknesses in control procedures as the assessment was performed by interviewing relevant officials and obtaining supporting evidence in line with the guidelines of the Archive NZs' Information Management (IM) Maturity Assessment.

The matters raised in this report are only those which came to our attention during the course of performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made. We cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud. Accordingly, management should not rely on our deliverable to identify all weaknesses that may exist in the systems and procedures under examination, or potential instances of non-compliance that may exist.

We have prepared this report solely for the use of Archives and Electoral Commission. The report contains constructive suggestions to improve some practices which we identified in the course of the review using the instructions and procedures defined by Archives. These procedures are designed to identify control weaknesses but cannot be relied upon to identify all weaknesses.

## 2. Executive Summary

### ELECTION COMMISSION

Te Kaitiaki Take Kōwhiri | Electoral Commission (EC) is an independent Crown entity, established in October 2010 and governed by the Electoral Act (the Act) 1993. EC's overall purpose is to provide an effective and impartial electoral system that New Zealanders understand and trust.

EC's core roles and responsibilities include:

- Running parliamentary elections (general elections, by-elections and referendums)
- Registering voters and adding them to the electoral roll
- Keeping confidence in the electoral system by staying neutral, upholding and following electoral law and working independently from government
- Educating New Zealanders about enrolling and voting
- Working with communities to help them understand and take part in elections, especially communities with low participation rates

The organisation holds high-risk/high-value records including statistical voting information.

The organisation has approximately 155 employees with its head office in Wellington and regional offices throughout the country. IM staff are integrated with the ICT team to provide IM and ICT services.

### SUMMARY OF FINDINGS

We assessed EC's IM maturity against the five maturity levels of Archives' IM Maturity Assessment model. The results are summarised below:

#### Maturity Level and Number of Findings

|                    |    |
|--------------------|----|
| <b>Beginning</b>   | 6  |
| <b>Progressing</b> | 13 |
| <b>Managing</b>    | 1  |
| <b>Maturing</b>    | 0  |
| <b>Optimising</b>  | 0  |

## 3. Introduction

### BACKGROUND

Archives provides IM leadership across the public sector. This is achieved through monitoring government organisations' IM practices to assure the New Zealand public that:

- Full and accurate records are created and maintained, improving business efficiency, accountability and government decision-making, and in turn, enhancing public trust and confidence in government;
- Government is open, transparent and accountable by making public sector IM practices known to the public.

Section 33 of the Public Records Act 2005 (PRA) requires that every public office has an independent audit of its record keeping practices every 5-10 years. The audit programme is part of Archives' monitoring and reporting on the state of public sector IM. It is one of the key components of their Monitoring Framework, which also includes an annual survey of public sector IM and the IM Maturity Assessment.

The Chief Archivist has commissioned Deloitte to undertake these audits of certain public offices and this audit was completed in October 2022.

### OBJECTIVE

To identify areas of IM strengths and weaknesses within the public office, prioritising areas that need attention and what needs to be done to strengthen them. These audits are seen as an important mechanism for organisations to improve their IM maturity and to work more efficiently and effectively.

### SCOPE

Deloitte has undertaken an independent point-in-time assessment of EC's IM practices against Archives' IM Maturity Assessment model. The IM Maturity Assessment aligns with the PRA and Archives' mandatory Information and Records Management standard. Topics 17 and 19 of the Archives IM Maturity Assessment are only applicable to local authorities and have therefore been excluded for the purposes of this audit.

The IM Maturity Assessment model classifies the maturity of IM practices from "Beginning" (least mature) to "Optimising" (highest maturity level). EC's maturity level for each topic area is highlighted under each of the respective areas. Ratings were based on the ENZ's officials' responses to questions during online interviews and the supporting documents provided in line with the IM Maturity Assessment guidelines.

Archives provided Deloitte with the framework including the specified audit plan, areas of focus for the PRA audits, and administrative support to Deloitte. Deloitte completed the onsite audit and audit report, which Archives reviewed before release to EC. Archives is responsible for following up on the report's recommendations with EC.

Our audit was based on a sample of IM systems, the review of selected documentation on a sample basis, and interviews conducted with a selection of staff and focus groups. As such, this audit does not relate to an Audit as defined under professional assurance standards.

The EC's feedback to this report is set out in Section 6.

## 4. Information Management Maturity Summary

This section lists the Information Management maturity level for each of the assessed topic areas. For further context refer to the relevant topic area in Section 5.

### ASSESSMENT MATURITY LEVEL

#### Governance

| No | Topic                                               | Beginning | Progressing | Managing | Maturing | Optimising |
|----|-----------------------------------------------------|-----------|-------------|----------|----------|------------|
| 1  | IM Strategy                                         |           | ●           |          |          |            |
| 2  | IM Policy                                           | ●         |             |          |          |            |
| 3  | Governance arrangements & Executive Sponsor         |           | ●           |          |          |            |
| 4  | IM Integration into business processes              |           | ●           |          |          |            |
| 5  | Outsourced functions and collaborative arrangements | ●         |             |          |          |            |
| 6  | Te Tiriti o Waitangi                                |           | ●           |          |          |            |

#### Self-monitoring

| No | Topic           | Beginning | Progressing | Managing | Maturing | Optimising |
|----|-----------------|-----------|-------------|----------|----------|------------|
| 7  | Self-monitoring |           | ●           |          |          |            |

#### Capability

| No | Topic                         | Beginning | Progressing | Managing | Maturing | Optimising |
|----|-------------------------------|-----------|-------------|----------|----------|------------|
| 8  | Capacity and Capability       |           | ●           |          |          |            |
| 9  | IM Roles and Responsibilities |           | ●           |          |          |            |

#### Creation

| No | Topic                               | Beginning | Progressing | Managing | Maturing | Optimising |
|----|-------------------------------------|-----------|-------------|----------|----------|------------|
| 10 | Creation and capture of information |           |             | ●        |          |            |
| 11 | High value / high-risk information  |           | ●           |          |          |            |

#### Management

| No | Topic                                         | Beginning | Progressing | Managing | Maturing | Optimising |
|----|-----------------------------------------------|-----------|-------------|----------|----------|------------|
| 12 | IM requirements built into technology systems |           | ●           |          |          |            |
| 13 | Integrity of information                      |           | ●           |          |          |            |
| 14 | Information maintenance and accessibility     |           | ●           |          |          |            |
| 15 | Business continuity and recovery              | ●         |             |          |          |            |

#### Storage

| No | Topic                            | Beginning | Progressing | Managing | Maturing | Optimising |
|----|----------------------------------|-----------|-------------|----------|----------|------------|
| 16 | Appropriate storage arrangements |           | ●           |          |          |            |

#### Access

| No | Topic                               | Beginning | Progressing | Managing | Maturing | Optimising |
|----|-------------------------------------|-----------|-------------|----------|----------|------------|
| 18 | Information access, use and sharing |           | ●           |          |          |            |

#### Disposal

| No | Topic                                              | Beginning | Progressing | Managing | Maturing | Optimising |
|----|----------------------------------------------------|-----------|-------------|----------|----------|------------|
| 20 | Current organisation-specific disposal authorities | ●         |             |          |          |            |
| 21 | Implementation of disposal decisions               | ●         |             |          |          |            |
| 22 | Transfer to Archives New Zealand                   | ●         |             |          |          |            |

**Note:** Topics 17 and 19 of the Archives IM Maturity Assessment are only applicable to local authorities and have therefore been excluded.

## 5. Audit Findings by Category and Topic

### GOVERNANCE

**The management of information is a discipline that needs to be owned 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

|                                                                                                                                                      |             |
|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| High-level statement outlining an organisation’s systematic approach to managing information across all operational environments of an organisation. | Progressing |
|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|

#### OBSERVATIONS

EC has a draft Data and Insights Strategy (the Strategy) that serves as its IM Strategy. The draft Strategy has some alignment to EC’s broader strategic direction and includes EC’s vision, success measures and key principles.

EC has a current Information Systems Strategy Plan (ISSP), approved in September 2021. The ISSP outlines key ISSP focus themes, frameworks and outcomes and aligns to EC’s broader strategy.

#### RECOMMENDATION

Finalise and approve the Strategy ensuring it follows Archives’ guidance and aligns with business needs.

#### Topic 2: IM Policy and Processes

|                                                                                                                                                              |           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| An information management policy supports the organisation’s information management strategy and provides a foundation for information management processes. | Beginning |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|

#### OBSERVATIONS

EC does not have an IM policy (the Policy) however, is currently drafting one. EC’s established IM processes are largely driven by the Act, privacy and security requirements but not the PRA.

There is a high-level awareness of the Act throughout EC and general awareness of the PRA and other relevant legislation such as, Privacy Act 2020, and Official Information Act (OIA) 1982. In addition, each business unit has established their own localised processes for managing information, as there is no Policy. Roles and responsibilities for IM are not outlined outside of a few business owners job descriptions.

EC recognises that high level policy guidance is an area in need of development.

#### RECOMMENDATION

Finalise and approve the Policy and ensure it references the PRA.

### Topic 3: Governance arrangements and Executive Sponsor

The Executive Sponsor has strategic and executive responsibility for overseeing the management of information in a public sector organisation.

Progressing

#### OBSERVATIONS

EC has a Data Stewardship Group (DSG) for IM related issues and is a formalised governance group with its own Terms of Reference. The DSG comprises of:

- Chief Electoral Advisor,
- Deputy Chief Executive,
- Manager of Legal and Policy,
- Chief Information Officer (CIO),
- Principal Advisor Data Insights.

Established in 2021, the DSG meets on a quarterly basis, unless urgent matters arise that require a special meeting.

The Chief Electoral/Executive Officer is EC's Executive Sponsor (ES) and provides IM guidance to the DSG but predominantly focusses on privacy and security incidents. There is no IM monitoring or reporting to DSG.

EC does not have any specific IM staff, instead, the CIO and the Senior Manager ICT Services are responsible for IM requirements.

#### RECOMMENDATION

Agree the IM reporting to be provided to the ES and DSG.

### Topic 4: IM Integration into Business Processes

All staff should be responsible for the information they create, use, and maintain. Business owners should be responsible for ensuring that the information created by their teams is integrated into business processes and activities. The IM team support business owners and staff.

Progressing

#### OBSERVATIONS

IM roles, responsibilities and requirements are sometimes identified and documented. Staff have a strong awareness around the security and privacy of all information that EC use and know who to contact in the event of an issue. Outside of these requirements, business owners, with the exception of ICT and Legal, have little awareness of their IM related responsibilities. ICT has some awareness of the PRA.

EC recently adopted SharePoint for its information management, but each business unit has their own informal file structures and naming conventions.

Outside of the Act requirements, integration of IM into business process and activities is well managed but subject to each team's individual processes due to the lack of IM Strategy and Policy.

#### RECOMMENDATION

Identify and ensure that IM requirements and responsibilities are integrated into IM documents and business processes.



## Topic 5: Outsourced Functions and Collaborative Arrangements

Outsourcing a business function or activity or establishing collaborative initiatives does not lessen an organisation’s responsibility to ensure that all requirements for the management of information are met.

Beginning

### OBSERVATIONS

ICT and Legal staff have a high awareness and understanding of the IM requirements of the contracts with the third parties. These include exit strategies, data ownership, information security, retention and disposal considerations. However, IM roles and responsibilities within each contract are not consistently outlined.

EC uses the Ministry of Business, and Innovation and Employment AoG contract template, which aligns with the PRA and other relevant legislation requirements. In addition, EC hold information sharing agreements with ministries. There is no regular monitoring of contracts to ensure compliance with the PRA.

Contractors are worked closely with on projects so are informally monitored as a result. There is currently no direct monitoring process to ensure IM requirements in contracts are met

### RECOMMENDATION

Develop a monitoring process to ensure IM requirements in contracts are met.

## Topic 6: Te Tiriti o Waitangi

The Public Records Act 2005 and the information and records management standard supports the rights of Māori under Te Tiriti o Waitangi/Treaty of Waitangi to access, use and reuse information that is important to Māori.

Progressing

### OBSERVATIONS

In August 2022, EC commissioned a Data Sovereignty Research review. Māori data and information was included as a key aspect.

EC, in response to the review, has since started to identify information of importance to Māori including significant amounts of personally identifiable data. This has resulted in a number of projects such as, improving Māori voting percentage, and working to strengthen relationships with iwi groups both regionally and nationally. This work has been championed alongside the Chief Māori Advisor.

Te Tiriti o Waitangi principles are incorporated and central to EC’s work.

### RECOMMENDATION

In consultation with the Chief Māori Advisor, formally identify all information of importance to Māori and document it within the Information Asset Register/Data Catalogue.

## 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 internal policies and processes.

### Topic 7: Self-Monitoring

Organisations should monitor all aspects of their information management.

Progressing

### OBSERVATIONS

EC's IM self-monitoring predominantly addresses the requirements in the Act. There is also monitoring of the information security, privacy and systems that EC use.

The requirements of the PRA and standard are not identified, documented and monitored. There is a general awareness of other legislative requirements among business owners. This is reflected in retention requirements, completing the ComplyWith survey and using and monitoring SharePoint. Generally, these requirements are not well documented.

### RECOMMENDATION

Identify and document IM requirements from the PRA and develop a review process to monitor compliance.

## 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

|                                                                                                      |             |
|------------------------------------------------------------------------------------------------------|-------------|
| Organisations should have IM staff or access to appropriate expertise to support their IM programme. | Progressing |
|------------------------------------------------------------------------------------------------------|-------------|

#### OBSERVATIONS

There are currently no IM roles in EC, however, the CIO and Senior Manager of ICT Services undertakes IM governance responsibilities.

EC staff have access to a professional development budget.

IM capability and capacity requirements for EC are limited. Following an external review of EC’s IM capability and capacity in August 2022, approval has been granted to employ a dedicated IM resource to address these capacity requirements.

#### RECOMMENDATION

Advertise and appoint to the approved IM role.

### Topic 9: IM Roles and Responsibilities

|                                                                                      |             |
|--------------------------------------------------------------------------------------|-------------|
| Staff and contractors should be aware of their responsibility to manage information. | Progressing |
|--------------------------------------------------------------------------------------|-------------|

#### OBSERVATIONS

All EC staff and contractors must comply with the Act requirements. EC’s IM considerations are influenced by the IM requirements in the Act and are well established and maintained. Outside of the Act, PRA related IM requirements are not actively considered or managed.

Staff are aware and sufficiently trained to meet these responsibilities alongside the importance of security and privacy information. Responsibilities under the PRA are not included in training, however, there is an awareness of the PRA and other relevant legislation across EC. SharePoint training is predominantly provided during onboarding however is limited to informal, business unit driven. SLT recognise that the use of SharePoint is new and challenging for some staff. A “SharePoint Champion” has been established to help with any staff members SharePoint issues.

For most staff, roles and responsibilities for IM are not outlined in their job descriptions or development plans, with the exceptions of Deputy Chief Executive, ICT and Legal.

There are generally, few IM training needs identified.

#### RECOMMENDATION

Identify training needed to address IM responsibilities and deliver to all staff during onboarding.

## 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

Every public office and local authority must create and maintain full and accurate information documenting its activities.

|          |
|----------|
| Managing |
|----------|

#### OBSERVATIONS

All staff understand and comply with the requirements of the Act and there is a general understanding of other legislative requirements including the PRA.

All staff have the capability to undertake the IM required by their role.

EC's SharePoint meets Archives' minimum metadata requirements. There is appropriate metadata routinely created to support usability and reliability of information. Access controls and permissions ensure that the information is controlled. Alongside SharePoint, EC's also uses Election management system as a core system during election periods. However, there is currently no monitoring of information usability or reliability on these systems.

EC does not have an organisation-wide naming convention and file management processes vary between business units. This can make it difficult for staff to find information from other business units.

Staff can and may be using local desktop/local storage to save documents, however there are mitigations in place to avoid this. This includes encouragement for sending SharePoint document links rather than attachments, limited local storage and IT system checking scripts sent out to Staff by ICT to check local storage use.

#### RECOMMENDATION

Develop and implement a plan for monitoring the creation and capture of information.

### Topic 11: High-Value/High-Risk Information

Staff and contractors should be aware of their responsibility to manage information. Every public office and local authority must create and maintain full and accurate information documenting its activities.

|             |
|-------------|
| Progressing |
|-------------|

#### OBSERVATIONS

There is a general awareness of the high-value/high-risk information that EC creates and is responsible for. This is predominantly driven from the Act requirements.

EC has an Information Asset Register (IAR) equivalent called the Data Catalogue that outlines systems, key information held in the system, and the business owner responsible. The Data Catalogue does not specify

which information is of high-value/high-risk to EC, the risks associated with the high-value information and the physical information that is in on-site physical storage or TIMG.

**RECOMMENDATION**

Finalise identifying all high-value/high-risk information and document in the Data Catalogue/IAR.

## MANAGEMENT

**Management of information should be designed into systems to ensure its ongoing management and access over time, including following a business disruption event. The 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 Solutions

|                                                                                                                |             |
|----------------------------------------------------------------------------------------------------------------|-------------|
| IM requirements must be identified, designed, and integrated into all of your organisation’s business systems. | Progressing |
|----------------------------------------------------------------------------------------------------------------|-------------|

#### OBSERVATIONS

Knowledge of the Act, privacy and security requirements are front of mind for managing information across EC staff. The Act requirements are identified and documented in all business changes and in contracts with third parties. Other PRA requirements have been considered, such as the retention requirements within SharePoint.

Outside of the Act requirements, as there is limited IM expertise at EC, aspects of IM are inconsistently managed during business changes.

The decommissioning of the onsite server and information transfer to SharePoint was managed by creating backups of all information during the change. Teams were allowed to identify information to be migrated to SharePoint. Preservation of data integrity, authorised changes or loss of metadata was ensured.

EC’s systems meet the metadata requirements to operate and meet business needs. Standard metadata aspects are selected for most systems including SharePoint.

#### RECOMMENDATION

Ensure system design and configurations are fully documented and maintained for all business systems.

### Topic 13: Integrity of Information

|                                                                                                                       |             |
|-----------------------------------------------------------------------------------------------------------------------|-------------|
| Information should be managed so that it is easy to find, retrieve and use, while also being secure and tamper-proof. | Progressing |
|-----------------------------------------------------------------------------------------------------------------------|-------------|

#### OBSERVATIONS

EC has high confidence in the integrity of all the information they create and maintain. There is a strong focus across all EC staff to ensure information is reliable and trustworthy. Due to the nature of their work and the Act requirements, staff have a good understanding of what information needs to be created and how it should be managed.

Staff noted variable experiences in finding and retrieving information. Each business unit and regional office have their own localised IM processes. However, usually information outside of someone’s own business unit can be retrieved though contacting a member of another business unit.

RECOMMENDATION

Document and implement standardised IM processes to support finding and retrieving information.

**Topic 14: Information Maintenance and Accessibility**

Information maintenance and accessibility cover strategies and processes that support the ongoing management and access to information over time.

|             |
|-------------|
| Progressing |
|-------------|

OBSERVATIONS

EC has strategies in place to manage and maintain digital information during business changes. All digital information is captured in systems that are regularly backed up to local or cloud services. EC prioritise using servers that are New Zealand based with the exception of SharePoint, which is located in Australia. The ICT team minimises technology obsolescence risks by ensuring that systems are updated as new versions are released.

For physical information, EC use on-site physical storage and a third-party commercial storage maintains a list of all EC documents stored there. Institutional knowledge of the physical information held in physical storage has decreased over time due to staff turnover. Furthermore, physical information is not included in their Data Catalogue.

RECOMMENDATION

Ensure digital continuity needs for digital information are identified and plans are in place to address these.

**Topic 15: Business Continuity and Recovery**

This covers the capability of the organisation to continue delivery of products or services, or recover the information needed to deliver products or services, at acceptable pre-defined levels following a business disruption event.

|           |
|-----------|
| Beginning |
|-----------|

OBSERVATIONS

EC has a current Business Continuity Plan (BCP) that was last updated in March 2022. The BCP includes critical systems for business functions, recovery plans, actions required for restoring digital information, and specific roles and responsibilities are outlined.

Internal systems are regularly backed up, access controls are in place and cyber security testing is regularly undertaken.

Critical information, physical or digital, for business continuity is not included in the BCP.

RECOMMENDATION

Ensure the BCP is up-to-date and include critical information needed for business continuity.

## 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

Appropriate storage arrangements for both physical and digital information ensures information remains accessible and usable throughout its life.

|             |
|-------------|
| Progressing |
|-------------|

#### OBSERVATIONS

All of EC's digital systems have appropriate access controls and restrictions in place. EC's main voting system is disabled outside of voting periods to restrict all access. SharePoint has standard access restrictions in place.

EC use a third-party for storing physical information who hold an index of all information stored.

Physical information is stored in one of the storage rooms in the main Wellington office, which includes fire safety, pest control and ventilation. All onsite physical information is stored in labelled boxes on shelves but there is no information index and the room itself has no specific recovery plan. All Wellington EC staff have unrestricted access to the physical document storage room.

EC have not identified information protection and security risks.

#### RECOMMENDATION

Information protection and security risks are identified, documented and regularly reported on to the IM governance group.



## ACCESS

Ongoing access to and use of information enables staff to do their jobs. To facilitate this, organisations will need mechanisms to support the findability and usability of information. Information and data that is shared between organisations is identified and managed.

### Topic 18: Information Access, Use and Sharing

Staff and contractors are able to easily find and access the information they need to do their work. Access controls for information is documented and consistently applied and managed. Metadata facilitates discovery and use of information. Information and data received or shared under information sharing agreements is managed according to IM policies and processes.

|             |
|-------------|
| Progressing |
|-------------|

#### OBSERVATIONS

EC applies access controls for digital information. These are in place across all digital systems, including restricting access to folders within SharePoint. Some staff reported difficulties with applying access restrictions to appropriate SharePoint files.

Staff generally do not have many difficulties finding information they need. Within each business unit there are informal IM processes, which are learnt through informal business unit inductions. Other induction training supports the requirements of the Act, privacy and security requirements that EC must follow. Staff will contact a member of the relevant business unit if they cannot find something.

EC regularly applies IM processes for incoming and outgoing data shared with external parties. EC routinely shares information for legislated purposes such as jury lists.

#### RECOMMENDATION

Ensure consistent use of a file plan across the organisation to support discovery of information in digital systems.

## DISPOSAL

**Disposal activity must be authorised by the Chief Archivist under the PRA. 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 (or have a deferral of transfer) and be determined as either “open access” or “restricted access”.**

### Topic 20: Current Organisation-Specific Disposal Authorities

This is about an organisation having its own specific disposal authority, not the implementation of the disposal actions authorised by the authority. It is not about the General Disposal Authorities.

Beginning

#### OBSERVATIONS

EC does not have a current and approved organisation-specific disposal authority (DA).

#### RECOMMENDATION

Develop an organisation-specific DA in line with the IAR for approval by Archives.

### Topic 21: Implementation of Disposal Decisions

This is about the implementation of disposal decisions, whether from organisation-specific disposal authorities or the General Disposal Authorities.

Beginning

#### OBSERVATIONS

As governed by the Act, the only disposal that EC undertakes are used and unused physical ballot papers after the voting period has ended. The disposal of this information is a legislatively mandated Crown process that is well managed and undertaken with multiple authorisations.

EC has a strong retention culture. There have been no reported instances of any disposal under the General Disposal Authorities (GDA).

EC's MIKE system has voting information dating back more than 20 years. Information in other EC systems such as, SharePoint is retained for seven years including emails. If staff delete information, this information is visible in the staff member's recycling bin for seven years as per the SharePoint settings.

#### RECOMMENDATION

Ensure that system design and configuration supports the retention of information of long-term use.

## Topic 22: Transfer to Archives New Zealand

Information of archival value, both physical or digital, should be regularly transferred to Archives or a deferral of transfer should be put in place.

|           |
|-----------|
| Beginning |
|-----------|

### OBSERVATIONS

EC has not identified information that is older than 25 years or of archival value.

### RECOMMENDATION

Once EC has developed their DA, identify information that is older than 25 years or of archival value to manage appropriately until it can be transferred to Archives.

## 6. Summary of Feedback

The Electoral Commission accepts the findings of this audit are accurate and that it provides a useful direction for improving its management of public records. The findings and recommendations will inform a work programme to address those recommendations. A new permanent position has been created to assist the Commission to improve its information management maturity.

# Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organisation”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organisation”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

Deloitte New Zealand brings together more than 1500 specialist professionals providing audit, tax, technology and systems, strategy and performance improvement, risk management, corporate finance, business recovery, forensic and accounting services. Our people are based in Auckland, Hamilton, Rotorua, Wellington, Christchurch, Queenstown and Dunedin, serving clients that range from New Zealand’s largest companies and public sector organisations to smaller businesses with ambition to grow. For more information about Deloitte in New Zealand, look to our website [www.deloitte.co.nz](http://www.deloitte.co.nz).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organisation”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2023 For information, contact Deloitte Global.

10 May 2023

Te Rua Mahara o te Kāwanatanga 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)

Karl Le Quesne  
Chief Executive  
Te Kaitiaki Take Kōwhiri Electoral  
Commission  
[Karl.LeQuesne@elections.govt.nz](mailto:Karl.LeQuesne@elections.govt.nz)

Tēnā koe Karl

## Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of Te Kaitiaki Take Kōwhiri Electoral Commission (EC) completed by Deloitte 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*

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. EC has reached 'Managing' in only one topic.

The report shows that the recent adoption of SharePoint was a significant IM development and has the potential to improve maturity in several areas. Consistent standards for use of SharePoint need to be implemented such as a file plan/taxonomy and agreed naming conventions to improve findability across the system.

Currently the system is reported as having the standard seven-year retention applied. This meets the retention requirements for some information but not all. The appraisal work undertaken to prepare for a disposal authority and IAR is needed to determine how long information needs to be retained. Obtaining a disposal authority and implementing routine disposal will complement the specific process for ballot paper disposal.

### **Prioritised recommendations**

The audit report lists 20 recommendations to improve your organisation's IM maturity.

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

### **What will happen next**

The audit report and this letter will be proactively released on the Archives website shortly. We would be grateful if you would advise of any redactions that your organisation considers are necessary 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. We have sent a feedback survey link for the attention of your Executive Sponsor in the accompanying email.

Nāku noa, nā



Anahera Morehu  
Chief Archivist

**Te Rua Mahara o te Kāwanatanga Archives New Zealand**

Cc The Chief Executive is also the Executive Sponsor

## APPENDIX

| Category               | Topic Number                                           | Auditor's Recommendation                                                                                        | Archive's Comments                                                                                                                                                 |
|------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Governance</b>      | 1: IM Strategy                                         | <i>Finalise and approve the Strategy ensuring it follows Archives' guidance and aligns with business needs.</i> | This strategy should address operational and corporate information and include a roadmap which will assist EC understand the specialist IM resourcing requirement. |
| <b>Governance</b>      | 2: IM Policy and Processes                             | <i>Finalise and approve the Policy and ensure it references the PRA.</i>                                        | A well communicated Policy will help consistency of understanding and practice across the organisation.                                                            |
| <b>Governance</b>      | 5: Outsourced Functions and Collaborative Arrangements | <i>Develop a monitoring process to ensure IM requirements in contracts are met.</i>                             | This is particularly important where public records are created and maintained.                                                                                    |
| <b>Self-Monitoring</b> | 7: Self-Monitoring                                     | <i>Identify and document IM requirements from the PRA and develop a review process to monitor compliance.</i>   | The results of the self-monitoring should be reported to the Executive Sponsor for discussion with the Data stewardship Group as relevant.                         |
| <b>Capability</b>      | 9: IM Roles and Responsibilities                       | <i>Identify training needed to address IM responsibilities and deliver to all staff during onboarding.</i>      | This would support the use of SharePoint and generally help to embed good IM practice consistently across the organisations including naming conventions.          |
| <b>Creation</b>        | 11: High-Value/High-Risk Information                   | <i>Finalise identifying all high-value/high-risk information and document in the Data Catalogue/IAR.</i>        | The EC's Data Catalogue is a good foundation to build on with systems, key information held in the systems and business owners already identified.                 |



| Category          | Topic Number                                           | Auditor's Recommendation                                                                               | Archive's Comments                                                                                                                                                                                                                   |
|-------------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Management</b> | 13: Integrity of Information                           | <i>Document and implement standardised IM processes to support finding and retrieving information.</i> | Staff will be more self-sufficient in finding information across the organisation if IM is standardised as appropriate. This includes consistent use of a file plan as recommended in Topic 18: Information Access, Use and Sharing. |
| <b>Disposal</b>   | 20: Current Organisation-Specific Disposal Authorities | <i>Develop an organisation-specific DA in line with the IAR with approval by Archives.</i>             | This will aid the understanding of how long information needs to be retained and prioritise management.                                                                                                                              |