Deloitte.

Te Whare Wānanga o Waikato
University of Waikato

Public Records Act 2005 Audit Report

Prepared for Te Rua Mahara o te Kāwanatanga
Archives New Zealand

September 2023

MAKING AN IMPACT THAT MATTERS since 1845

Table of Contents

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 the University of Waikato. 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 the University of Waikato 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 the University of Waikato. 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

TE WHARE WĀNANGA O WAIKATO | UNIVERSITY OF WAIKATO

Te Whare Wānanga o Waikato | University of Waikato (the University) is a tertiary education organisation (TEO) with the overall purpose to educate and conduct research. It was established on 1 January 1964, by the University of Waikato Act 1963 (the Act) and is governed by the Education and Training Act 2020.

The mission of the University is to combine the creation of knowledge through research, scholarship and creative works with the dissemination of knowledge through teaching, publication and performance.

With its principal campus located in Hamilton and secondary campuses in Tauranga and Hangzhou China, the University employs approximately 1,500 staff with approximately 13,000 enrolled students.

The University's high-risk/high-value records include:

- Student's academic final results
- Scholarship establishment
- Honorary degree conferment
- Large capital expenditure construction and engineering projects
- Council and strategic committee meetings
- University identity, brand, and image
- High level governance contracts and agreements
- Publications produced or commissioned by the University
- Patent registration and intellectual property ownership.

The Executive Sponsor (ES) is the University Librarian and a member of the IM team. The IM team consists of the ES, Records Manager, Associate Director of Infrastructure and Security, and the Director of the Vice-Chancellor's Office. This group also forms the Information Governance Group (IGG).

SUMMARY OF FINDINGS

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

Maturity Level and Number of Findings

Beginning	2
Progressing	13
Managing	5
Maturing	0
Optimising	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 April 2023.

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 the IM practices at the University against Archives' IM Maturity Assessment model. The IM Maturity Assessment aligns with the PRA and Archives' mandatory Information and records management standard (the 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). the University 's maturity level for each topic area is highlighted under each of the respective areas. Ratings were based on the University's staff 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 the University. Archives is responsible for following up on the report's recommendations with the University.

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 University'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		●			

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.	Beginning

OBSERVATIONS

The University does not have an IM Strategy, which the Information Governance Group (IGG) plans to address based on the findings and recommendations in this report.

RECOMMENDATION

Develop and approve an IM Strategy to provide long-term organisation-wide direction for IM in order to meet business requirements.

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.	Managing

OBSERVATIONS

The Records Management Policy (the Policy) was approved in 2019 and is due to be reviewed in 2024 to ensure it remains relevant. The Policy sets out high-level IM principles which all staff are required to comply with as per the University's Code of Conduct. In addition, the Policy outlines IM roles and responsibilities with specific reference to the PRA and other relevant legislation.

An additional guide that outlines IM requirements is the Records Management Procedures document (RM Procedures) which aligns with the Policy. Both resources are available through the University's website; the Policy is publicly available while the RM Procedures are restricted to staff with login privileges.

The RM Procedures include guidance documents on security, retention, disposal, information classification, emails, and the archiving of records. However, it does not outline consistent IM practice across the organisation due to the variety of business activities which produce several record types across different systems. This results in differing localised IM processes across each business unit.

Staff interviewed have varying levels of awareness of their IM roles and responsibilities, the Policy and the RM Procedures. However, there was a general awareness of the PRA and other relevant legislation such as the Privacy Act 2020 and the Official Information Act 1982. This legislative awareness comes from the

requirement for staff to review relevant policies and procedures and confirm their understanding by signing the Code of Conduct during induction.

RECOMMENDATION

Develop and document localised IM practises for each business unit to align with their systems and processes, ensuring all IM responsibilities are integrated and met.

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

The ES is the University Librarian and a member of the IGG, which meets monthly and supports the Vice-Chancellor with IM related oversight. The IGG's Terms of Reference sets out the IM responsibilities, however, outside of meeting minutes there is no requirement for regular, formal monitoring or reporting.

The ES performs their role through supporting the development of IM documentation and communicating the importance of IM to the IGG group and across the organisation.

RECOMMENDATION

Identify and agree areas of IM to be monitored and reported to the IGG.

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

Business owners are responsible for ensuring that IM requirements are met. Many University staff have knowledge of their IM responsibilities from their role-specific requirements, however this was not consistent across all interviewed staff. IM responsibilities are integrated into most business processes. Staff were aware of their obligations around security and privacy of information and who to contact when an event or breach occurred.

The main digital storage systems at the University are the local shared network drives and an electronic document management system (EDMS). Each business unit has their own localised naming conventions and file structures and utilises one or both systems for their own purposes. In addition, some business units have their own specific systems which also have stored information. This creates a challenge for the University to have clear oversight and monitoring of IM processes across different business units and systems.

To ensure there are not multiple copies of information in the various systems, the University has adopted an 'Authoritative Record' designation. As explained in the RM Procedures, 'only one copy of a record must be held by the University, and this is referred to as the authoritative record'. The authoritative record is held by the information creator or the process owner. Staff interviewed, had varying knowledge and application of the 'Authoritative Record' designation.

In the second half of 2023, the University is migrating workspaces and as part of this is planning to rationalise the shared network drives and the current EDMS onto one EDMS.

RECOMMENDATION

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

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.	Progressing

OBSERVATIONS

The legal team is responsible for managing the contract management system which includes general contract monitoring and the oversight of other service agreements. This monitoring of contractual compliance does not include an assessment of whether IM requirements are met.

The University has its own template to guide the structure of all contractual agreements. Most contracts set the requirement to align with the University policies. This includes requirements to meet privacy, ownership, and security responsibilities, but IM obligations and responsibilities are not explicitly stated.

The reviewed agreements set the expectation of compliance with New Zealand legislation, but no specific reference is made to the PRA.

RECOMMENDATION

Ensure IM requirements, and roles and responsibilities are explicitly included in contracts for outsourced functions and collaborative arrangements.

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.	Managing

OBSERVATIONS

The University and the IGG have a good understanding of their Te Tiriti o Waitangi settlement agreements. A kaitiaki approach is taken in the management of all Māori and Te Tiriti information.

There is good awareness of the information that is of importance to Māori. For example, a significant amount of the University's physical information has been classified as taonga. This has been indexed in the physical records management system.

The University is aware of their data sovereignty challenges when storing sensitive digital Māori information within their current EDMS due to its storage location being in Singapore. To avoid this issue, most sensitive digital Māori data is stored in local shared networks with access being restricted to authorised staff. Currently, sensitive and non-sensitive Māori information is only stored temporarily in the EDMS or if access is required due to collaboration purposes. Once the collaboration is finished, the information is saved to the local University network and its user access is removed in the EDMS. The University is aware that this is still

an issue as the information remains in the EDMS back-ups and are looking to address this in their migration to a new EDMS.

RECOMMENDATION

Improve accessibility and discoverability of information of importance to Māori.

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

The University uses a third-party legislative compliance monitoring tool, to annually monitor its PRA requirements.

Senior management provides IM support and ad hoc advice when requested. Currently there is no formal monitoring of the University's IM responsibilities and systems.

The IGG is creating a plan to implement regular check-ins with business owners. These check-ins are intended to provide support through ensuring that PRA and IM requirements are complied with. This will also create an opportunity for the IGG to provide guidance and address any IM related issues within the different teams.

RECOMMENDATION

Develop and implement a process to regularly monitor and review IM compliance with the Policy and RM Procedures across the different business units to encourage consistency of practice.

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

The Records Manager, with oversight of the ES, oversees and manages IM by championing, implementing, reviewing and updating IM policy and process documents. The Director of the Vice-Chancellor's Office provides advice and assurance on IM related issues to the IGG and together with the ES shares the responsibility of escalating outcomes to SLT if necessary. As an additional support, the Associate Director of Networks, Security and Assurance provides ICT oversight, and management of digital systems.

There currently is limited IM capacity and capability within the IM team and wider University. The IM team is aware of the additional resources required to enable sufficient IM support for digital information.

To increase the current IM capability levels within the University, there is a professional development budget available. This budget is not IM specific, however IM specific training can be requested.

RECOMMENDATION

Ensure that IM capability and capacity is regularly assessed and appropriately resourced to address business needs.

Topic 9: IM Roles and Responsibilities

Staff and contractors should be aware of their responsibility to manage information.	Beginning

OBSERVATIONS

The Policy includes IM roles and responsibilities for staff and contractors. This information is also included in relevant job descriptions and performance plans but not for all the University staff. There are also requirements around compliance with the University policies and relevant New Zealand legislation, which includes the PRA.

The current onboarding training provided to staff and contractors is not formalised or standardised across the business due to the variety of systems and processes across business units. Any onboarding provided by managers is business unit specific. IM roles and responsibilities for managing the information they create and maintain is not included. Some staff have awareness of their IM responsibilities, but this is either attributed to previous role experience or is a current component of their role.

RECOMMENDATION

Create a standardised and mandatory IM induction programme for all relevant staff and contractors.

CREATION

It is important to take a systematic approach to the management of government information, and this starts with an understanding of what information must be created and captured. It is expected that public offices create and capture complete and accurate documentation of the policies, actions, and transactions of government. Knowing what information assets are held by public offices is essential to IM practice.

Topic 10: Creation and Capture of Information

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

OBSERVATIONS

There is some general understanding and compliance with requirements to create and capture information. Staff interviewed stated that information was saved in the correct place as directed by their business unit.

The IM team is responsible for overseeing the process of creating and managing physical information. The IM team periodically reminds staff of their responsibilities for identifying, (including labelling and naming), filling, retaining, destroying (annually if appropriate) and storing physical information.

There are no controls in place to prevent digital information being stored on local networked desktops, although this information, and information stored within the EDMS's cloud storage, is backed up.

Most current systems at the University meet Archives' metadata requirements but not all. While the current EDMS meets metadata requirements, the local network drive does not. The planned new EDMS will be configured to ensure Archives' metadata requirements are met.

There are no established file naming conventions at the University as naming conventions vary across computer operating systems. The file management processes tend to vary between business units which sometimes creates challenges for staff to locate information. This is intended to be addressed with the new EDMS including naming guidelines.

RECOMMENDATION

Ensure that the planned new EDMS meets Archives' minimum metadata requirements.

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

Staff have a good awareness of the high-value/high-risk information created by the different business units.

The Information Security Classification (ISC) is similar to an Information Asset Register (IAR) at the University. The ISC outlines the systems and key information stored in each system. Details are provided around the responsible business owner, information classifications and a risk matrix. The last ISC update was in 2021.

RECOMMENDATION

Assess if further work is required to utilise the ISC as an IAR and plan how this will be done.

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

With the upcoming implementation of the new EDMS, the IGG will work closely with the ICT team to ensure IM requirements are built into the system.

The University has strategies and processes in place to manage the risk of business disruption during major digital information projects. IM relevant business changes are managed in house by ICT with the assistance of third-party specialists who provide additional support as required.

A recent transition to a new system demonstrated the effectiveness of the processes used during a business change. The preservation of data and the prevention of metadata loss was ensured. While this was sufficiently managed, there are no requirements for business units to document system designs and configurations.

RECOMMENDATION

Ensure that IM expertise is involved in the design and configuration decisions for the new EDMS so that IM requirements are met.

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

The University is confident in its processes for creating and storing information. There are many localised IM practices built into the University's systems that ensure that information is reliable and trustworthy within each business unit. For example, version controls in EDMS and system access controls.

Staff stated they had variable experiences in locating and retrieving information due to the varying systems and privacy and security access restrictions in place. If information is required from another business unit, this is usually retrieved through contacting a member of the business unit.

RECOMMENDATION

Assess the issues with finding and retrieving information across the organisation and implement solutions.

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.	Managing

OBSERVATIONS

The shared network drives are stored on-site. All information access is restricted to relevant role requirements and any security incidents are reported to the ICT team and the ES.

The University has two main physical storage locations. The primary location is an on-site storage facility, which the University owns, and the IM team manages. The second location is on campus and used by the Vice-Chancellor's Office to store high-value/high-risk confidential and restricted information. An SLT member manages all access to this room.

All physical information is managed through the physical record management system which maintains a current index of all information.

Technology obsolescence risks have been formally identified and plans are under development to address these. All digital information is captured in systems that are regularly backed up to local or cloud services. Access controls, security processes and continuous system updates provides some assurance that digital information remain accessible over time.

RECOMMENDATION

Ensure digital continuity strategies for digital and physical information are incorporated into business planning and change.

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.	Progressing

OBSERVATIONS

The University has a hierarchy of Business Continuity Management (BCM) documents. This hierarchy includes a Business Continuity Plan (BCP) Strategy, BCP Policy, desktop guides, decision-making guide, and business unit specific BCPs. The relevant IM BCP's include the ICT Disaster Recovery Plan and the Library's BCP.

The Library's BCP accompanies the Library's Business Impact Analysis document to cover physical information and the physical records management system. These two policies outline the priority ratings of critical functions, activities, roles and responsibilities in an event, and critical activities.

The Library's BCP was updated in 2020 and tested in the same year with the Business Impact Analysis undertaken in 2021. Both documents are set for review every three years. Internal systems are regularly backed up to ensure information can be restored following a business disruption event. Cyber security testing is regularly undertaken by third parties.

The ICT Disaster Recovery Plan which covers digital information, was last updated in 2015 and is due for a review. It includes critical systems for business functions, disaster recovery plans, actions required for restoring digital information, and specific roles and responsibilities.

RECOMMENDATION

Ensure the ICT Disaster Recovery Plan is up-to-date and includes current critical information and systems 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.	Managing

OBSERVATIONS

As previously mentioned, the current cloud based EDMS is stored in Singapore, and the requirements for information security and protection are included in the respective service contracts.

The University building used to store the Vice-Chancellor's Office physical information has been closed, with the current storage location considered a temporary one.

The current locations have controls such as fire safety, flood mitigation, pest control and ventilation. All onsite physical information is stored in labelled boxes on shelves with high-risk/high-value information separately secured in a locked cabinet with restricted access. Each storage location has its own storage checklist document outlining the review date, storage availability, privacy and security, protection and preservation, and identification and accessibility.

The University recognises that the current locations do not meet all of its storage requirements, such as desirable humidity levels with an available air conditioning unit. The University plans to address this through relocating all physical documentation into one adequate storage location in the last quarter of 2023.

RECOMMENDATION

Ensure that the new physical storage location meets all of Archives' storage requirements.

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

The University applies access controls for both physical and digital information. Access controls are in place across all digital systems, including restricting access to digital information based on role requirements. However, some staff commented that previously granted role-specific access was not revoked after starting a new role. This issue has been raised in previous IT audits with access controls and permissions found to not be monitored.

There is little oversight and monitoring of information usage and data sharing agreements with third parties, due to the varying localised processes and systems across the University.

The University's current systems do not meet the minimum Archives' metadata requirements, specifically the two main shared drives. Additional metadata is not added to any core digital storage systems, but metadata is added to the physical records management system.

Most staff reported issues with the findability of information, naming conventions, version control and taxonomy of digital information. These issues were emphasised when information was required to be located and retrieved outside of the business unit.

As previously mentioned, all physical information is stored on-site and is identified and managed through the use of the University's physical information document management system. Staff can request retrieval of physical information through the IM team as needed.

RECOMMENDATION

Identify risks to information from current IM practices including access controls, use, sharing and discovery of information and developing appropriate mitigations.

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.	Managing

OBSERVATIONS

The University has a current and approved disposal authority (DA). DA702 covers the eight New Zealand Universities and is due for review in seven years. Approved in July 2021, it is reviewed every 10 years with its next review scheduled for 2031. The DA covers all of the University's business functions and formats for their core information.

RECOMMENDATION

Ensure there is a regular internal review cycle for the DA.

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.	Progressing

OBSERVATIONS

Staff interviewed had different levels of awareness of the DA and GDA's requirements. Some staff noted that they receive an annual disposal email reminder. The IM team has also created the Records Disposal Guidelines document on the staff intranet to provide guidance around the disposal process. The annual disposal email and the Records Disposal Guidelines focus on the disposal of physical information but not digital information.

Each year, the IM team identifies, and reviews physical records registered in the physical records management system under the GDAs and DA, that have reached the end of their minimum retention period. These records are destroyed onsite by a storage service provider.

A disposal register can be extracted from the physical records management system. It includes the document name, owner, department, classification, description, and open and close date.

The University has not identified or established a process to dispose of relevant digital information.

RECOMMENDATION

Create a disposal implementation plan for both physical and digital information.

Topic 22: Transfer to Archives

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

OBSERVATIONS

The University has identified all physical information that is over 25 years old and in scope for transfer. This process occurs every five years and the University has an index of all previous information transferred to Archives. The last transfer of physical information to Archives was in 2019.

In comparison, digital information that is over 25 years old has not been identified across all systems.

RECOMMENDATION

Identify digital information that is older than 25 years or of archival value and engage with Archives over potential transfer.

6. Summary of Feedback

The University of Waikato - Te Whare Wānanga o Waikato wishes to thank Archives New Zealand and Deloitte for the opportunity to participate in the Public Records Act 2005 audit process and for the constructive manner in which the audit was conducted. Waikato is committed to continuous improvement in our information and records management arrangements and will use the audit report to prioritise future developments.

Deloitte.

Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND

27 October 2023

Te Rua Mahara o te Kāwanatanga Archives New Zealand
10 Mulgrave Street
Wellington
Phone +64 499 5595
Websites www.archives.govt.nz
www.dia.govt.nz

Neil Quigley
Vice-Chancellor
Te Whare Wānanga o Waikato University of Waikato
Neil.quigley@waikato.ac.nz

Tēnā koe Neil

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of Te Whare Wānanga o Waikato University of Waikato (the University) 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 (Te Rua Mahara) is mandated by the PRA to regulate public sector information management (IM). The audit programme is a key regulatory tool in our Monitoring Framework.

Monitoring IM practice across the public sector gives assurance that the government is open, transparent and accountable by providing visibility of public sector IM practices. Full, accurate and accessible information improves business efficiency and government decision-making and accountability, which in turn enhances public trust and confidence. Information that is well managed unlocks the value of government information for the benefit of everyone.

We are confident that you and your organisation are committed to delivering high-quality, trusted information to decision-makers, other government organisations, customers and stakeholders. We trust that the audit process will support this commitment. The audit report and this letter recommend changes to support improvement of your organisation's IM practices.

Audit findings

In the audit report, the auditor has independently assessed your information maturity against the framework of our IM Maturity Assessment. Prior to the audit, your organisation completed the Maturity Assessment. This provided a self-assessment of IM maturity for your own use and as context for the auditor about your organisation.

Organisations that are assessed as having a maturity level of 'Managing' across all IM topics are broadly meeting the minimum requirements expected by the PRA and our mandatory Information and records management standard. The University's IM is assessed as operating mostly at 'Progressing' maturity.

Implementation of a new electronic document management system (EDMS) has the potential to improve IM maturity across several topics. If set up well it will improve user issues with finding and retrieving information (as identified in Topic 13: *Integrity of Information* and Topic 18*: Information Access, Use and Sharing).* The EDMS also presents the opportunity for disposal of digital information as part of the migration activity and within the system itself. The University does well with physical information disposal and will be able to better manage digital disposal in the new environment.

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 our 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
Poumanaaki Chief Archivist
Te Rua Mahara o te Kāwanatanga Archives New Zealand

Cc Michelle Blake, University Librarian (Executive Sponsor), michelle.blake@waikato.ac.nz

APPENDIX

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Governance	1: IM Strategy	*Develop and approve an IM Strategy to provide long-term organisation-wide direction for IM in order to meet business requirements.*	This strategy will provide direction for the University's IM development and to understand the associated resourcing required to implement improvement activities. Information and records management strategy
Governance	3: Governance Arrangement and Executive Sponsor	*Identify and agree areas of IM to be monitored and reported to the IGG.*	Implementing agreed monitoring will help the IGG better understand issues concerning IM and prioritise improvement activity. This also addresses the recommendation for Topic 7: *Self-Monitoring.*
Governance	4: IM Integration into Business Processes	*Responsibility for managing information within business units is consistently assigned to business owners.*	Good awareness of their IM role and responsibilities means that business owners can effectively support their staff with oversight from IM specialists.
Capability	8: Capacity and Capability	*Ensure that IM capability and capacity is regularly assessed and appropriately resourced to address business needs.*	IM resourcing requirements needed to implement the IM Strategy roadmap should be understood as well as the resourcing needed to meet BAU requirements.
Capability	9: IM Roles and Responsibilities	*Create a standardised and mandatory IM induction programme for all relevant staff and contractors.*	Staff and contractors must understand what their IM roles and responsibilities are at the start of their employment. IM induction training ensures that all staff understand what IM is required.

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Creation	11: High-Value/High-Risk Information	*Assess if further work is required to utilise the ISC as an IAR and plan how this will be done.*	If the ISC is system-based, then this might not be suitable as an IAR as information assets may be held across different systems. This would be a good exercise to share the approach taken with other universities.
Management	12: IM Requirements built into Technology Solutions	*Ensure that IM expertise is involved in the design and configuration decisions for the new EDMS so that IM requirements are met.*	The design of the new EDMS is the optimum time to ensure that all IM requirements are included in the new system which will result in a maturity lift in other topics as well. This requires collaboration of ICT with IM experts.
Storage	16: Appropriate Storage Arrangements	*Ensure that the new physical storage location meets all of Archives' storage requirements.*	This is especially important for information of archival value. The University needs to consider the length of time that storage is needed outside of transfer to the Auckland regional repository of Te Rua Mahara.