KPMG

Public Records Audit Report for Auckland University of Technology

Prepared for Te Rua Mahara o te Kāwanatanga Archives New Zealand

September 2023

kpmg.com/nz

Disclaimers

Inherent Limitations

This report has been prepared in accordance with our Consultancy Services Order with Te Rua Mahara o te Kāwanatanga Archives New Zealand (Te Rua Mahara) dated 26 November 2020. Unless stated otherwise in the CSO, this report is not to be shared with third parties. However, we are aware that you may wish to disclose to central agencies and/or relevant Ministers' offices elements of any report we provide to you under the terms of this engagement. In this event, we will not require central agencies or relevant Ministers' offices to sign any separate waivers.

The services provided under our CSO ('Services') have not been undertaken in accordance with any auditing, review or assurance standards. The term "Audit/Review" used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The information presented in this report is based on that made available to us in the course of our work, publicly available information, and information provided by Te Rua Mahara and the Auckland University of Technology. We have indicated within this report the sources of the information provided. Unless otherwise stated in this report, we have relied upon the truth, accuracy and completeness of any information provided or made available to us in connection with the Services without independently verifying it.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, the Auckland University of Technology management and personnel consulted as part of the process.

Third Party Reliance

This report is solely for the purpose set out in Section 2 and 3 of this report and for Te Rua Mahara and Auckland University of Technology's information, and is not to be used for any other purpose or copied, distributed or quoted whether in whole or in part to any other party without KPMG's prior written consent. Other than our responsibility to Te Rua Mahara, neither KPMG nor any member or employee of KPMG assumes any responsibility, or liability of any kind, to any third party in connection with the provision of this report. Accordingly, any third party choosing to rely on this report does so at their own risk. Additionally, we reserve the right but not the obligation to update our report or to revise the information contained therein because of events and transactions occurring subsequent to the date of this report.

Independence

We are independent of Te Rua Mahara in accordance with the independence requirements of the Public Records Act (PRA) 2005.

Contents

1. Executive summary

Established in 2000, Auckland University of Technology (AUT) is a public university in New Zealand, hosting nearly 30,000 students across three campuses in Auckland.

AUT creates and maintains high-value public records in relation to:

- Qualifications and academic records of students
- Records of programmes and courses
- Student administration
- Audit and governance documents
- Board and committee meeting minutes, including those of AUT's Council
- Historic documents from the founding of AUT.

AUT maintains its information on various systems including a student management system, financial management system, payroll and human resources system, and Microsoft 365 (e.g. SharePoint, Teams, Word and Outlook).

AUT employs 2249 full-time staff. Following a decentralised approach to information management, responsibility for information management is delegated to AUT's various service divisions and faculties. AUT's Records Management team, led by the Group Director, Risk and Assurance, comprises an Information Management (IM) Consultant and an Information Technology (IT) Manager. Nine staff form the Data and Information Governance Group (DIGG) which provides the framework and guidance to ensure AUT meets its Public Records Act (PRA) requirements.

AUT maintains a mix of physical and digital information and uses a third-party provider for storage and destruction of physical information.

AUT's information management maturity is summarised below. Further detail on each of the maturity assessments can be found in Sections 4 and 5 of this report.

Beginning	**3**
Progressing	**13**
Managing	**3**
Maturing	**1**
Optimising	**0**

2. Introduction

KPMG was commissioned by Te Rua Mahara to undertake an independent audit of AUT under section 33 of the PRA. The audit took place in May 2023.

AUT's information management (IM) practices were audited against the PRA and the requirements in the Information and records management standard (the Standard) as set out in the Information Management (IM) Maturity Assessment of Te Rua Mahara.

Te Rua Mahara provides the framework and specifies the audit plan and areas of focus for auditors. Te Rua Mahara also provides administrative support for the auditors as they undertake the independent component of the audit process. The auditors are primarily responsible for the onsite audit, assessing against the Standard, and writing the audit report. Te Rua Mahara is responsible for following up on the report's recommendations with your organisation.

3. This audit

This audit covers all public records held by AUT including both physical and digital information. AUT Ventures Limited is a wholly owned subsidiary of AUT. AUT does not provide information services to AUT Ventures, so it was out of scope for the audit.

The audit involved reviews of selected documentation, interviews with selected staff, including the Executive Sponsor, information management staff, the information technology team, and a sample of other staff members from various areas of AUT. Note that the Executive Sponsor is the Senior Responsible Officer for the audit.

The audit reviewed AUT's information management practices against the PRA and the requirements in the Standard and provides an assessment of current state maturity. As part of this audit, we completed systems assessments over AUT's SharePoint, student management system, payroll and human resources system, and management reporting and business intelligence system. Where recommendations have been made, these are intended to strengthen the current state of maturity or to assist with moving to the next level of maturity.

The summary of maturity ratings can be found at Section 4, with detailed findings and recommendations following in Section 5. AUT has reviewed the draft report, and a summary of its comments can be found in Section 6.

4. Maturity Assessment

This section lists all assessed maturity levels by topic area in a table format, refer to Appendix 1 for an accessible description of the table. For further context about how each maturity level assessment has been made, refer to the relevant topic area in the report in Section 5.

Category	No.	Topic	Maturity				
			Beginning	Progressing	Managing	Maturing	Optimising
Governance							
	1	IM strategy				●	
	2	IM policy and processes			●		
	3	Governance arrangements and Executive Sponsor			●		
	4	IM integration into business processes		●			
	5	Outsourced functions and collaborative arrangements		●			
	6	Te Tiriti o Waitangi	●				
Self-monitoring							
	7	Self-monitoring		●			
Capability							
	8	Capacity and capability		●			
	9	IM roles and responsibilities		●			
Creation							
	10	Creation and capture of information		●			
	11	High-value / high-risk information		●			
Management							
	12	IM requirements built into technology systems		●			
	13	Integrity of information		●			
	14	Information maintenance and accessibility		●			
	15	Business continuity and recovery		●			
Storage							
	16	Appropriate storage arrangements		●			
Access							
	18	Information access, use and sharing		●			
Disposal							
	20	Current organisation-specific disposal authorities			●		
	21	Implementation of disposal decisions	●				
	22	Transfer to Te Rua Mahara	●				

Please note: Topics 17 and 19 in the Information Management Maturity Assessment are applicable to local authorities only and have therefore not been assessed.

5. Audit findings by category and topic

Governance

The management of information is a discipline that needs to be owned from the top down within a public office. The topics covered in the governance category are those that need senior-level vision and support to ensure that government information is managed to ensure effective business outcomes for the public office, our government, and New Zealanders.

TOPIC 1 – IM strategy — Maturing

Summary of findings

AUT has an information management strategy called the 'Information Management Strategy and Roadmap' (the Strategy). The Strategy outlines strategic direction for 2023 - 2025. It includes sections specifically relating to strategy, as well as maturity gaps and improvement initiatives. It was endorsed by the Data and Information Group (DIGG) whose membership is made up of senior management at AUT, including the Executive Sponsor.

The Strategy supports business needs for information management by assessing the current state maturity and outlining a series of maturity targets. The Strategy aligns with the requirements of the IM Maturity Assessment.

There is evidence of regular review and reporting against progress of the Strategy during DIGG meetings. The 'DIGG Information Management Roadmap 2023 - 2025' supports the Strategy as it outlines key strategic initiatives along a timeline. Updates on these initiatives provided during DIGG meetings enable DIGG to track progress.

The Strategy has been communicated to staff and contractors via AUT's intranet. It underpins AUT's strategic direction and aligns with organisational data and information goals.

Recommendation

Ensure the Strategy is regularly reviewed and updated to reflect changing business needs and direction.

TOPIC 2 – IM policy and processes — Managing

Summary of findings

AUT has a current information management policy called the 'Records Management Policy' (the Policy) that was recently approved by the Vice-Chancellor. It links to relevant legislation and the Standard, as well as other internal policies. This includes the Information and Communication Technology Policy, Information and Communication Technology Procedures and Information Sensitivity Guidelines.

There are up-to-date, approved, and documented processes which support the Policy called the 'Records Management Procedures' (the Procedures). These processes aim to ensure a consistent approach to the creation, management and disposal of information, supporting both organisational initiatives and compliance under the PRA. However, these processes are not actively built into all information systems and business processes.

The Policy and Procedures are communicated and available to all staff via the intranet. In accordance with standard AUT practice as it is a new policy, staff were being informed of its contents at the time of the audit. The Policy documents roles and responsibilities. However, information management is not included in job descriptions for all staff.

Recommendation

Ensure the Policy and Procedures are actively built into all information systems and business processes.

TOPIC 3 – Governance arrangements and Executive Sponsor — Managing

Summary of findings

The DIGG is AUT's information management governance group. The DIGG is chaired by the Chief Technology Officer and Chief Information Security Officer (CISO) and meets at least quarterly. Membership is comprised of senior management from across AUT. In addition, there are two Sub Committees leading workstreams relating to research and administrative data, which report to DIGG.

Through interviews it was noted that the Executive Sponsor provides appropriate support on any information management issues and is a role model for good information management practices. The Executive Sponsor provides regular updates to the Vice-Chancellor and the DIGG reports to AUT's Executive Leadership Team (ELT) on an annual basis. DIGG was established in May 2021 with the first formal report provided to the Executive Leadership Team in December 2022.

There is evidence of some information management reporting at DIGG meetings. For example, the Director Data, Technology, Risk & Policy has provided progress updates and changes to the roadmap have been discussed.

Recommendation

Decide what information management activity needs regular monitoring. Implement a plan to report on it to DIGG via the Executive Sponsor.

TOPIC 4 – IM integration into business processes — Progressing

Summary of findings

Information management responsibilities for all AUT staff are well documented in the Records Management Policy and Records Management Procedures, but no formal training on these responsibilities is currently provided. Staff interviewed noted the need for training on information management responsibilities to ensure these are applied to business-as-usual activity.

Requirements for managing information are integrated into business processes. For example, the recent implementation of a service management system in the People and Culture team incorporated records and information management practices to ensure that staff created complete and accurate information. The system forms an integral part of managing employee records such as logging requests to change or update employee information. In addition, the system is only accessible by appropriate staff and time stamps information.

Recommendation

Provide information management training to business owners to increase their understanding of information management responsibilities.

TOPIC 5 – Outsourced functions and collaborative arrangements — Progressing

Summary of findings

Requirements for managing information are outlined in some, but not all contracts where there are outsourced functions or collaborative arrangements. Three contracts were sampled during the audit. One contract related to the provision of pastoral care services to AUT. Public records created on behalf of AUT under this contract include records relating to critical incident management.

The three contracts sampled did not contain clauses recognising the public record status of the records the contracted parties were expected to provide. AUT relies on the requirement of contracted parties to comply with New Zealand law, as stated within the contracts sampled, to help ensure compliance with the PRA. All contracts sampled addressed either information ownership or intellectual property in the records created. For example, under one of the contracts, the parties agreed to assign all data and information ownership rights to AUT for data and information arising from services rendered in connection with the contract.

Monitoring of contracted parties to ensure information management requirements are met is limited. If staff do not receive all required information at the end of a contract, they will request

the missing information from the contracted party. However, there is no structured process for monitoring compliance against information management requirements.

Recommendations

Develop a process to monitor the compliance of contracted parties in relation to their information management requirements.

Ensure all contracts for outsourced functions or collaborative arrangements include information management requirements, roles and responsibilities.

TOPIC 6 – Te Tiriti o Waitangi — Beginning

Summary of findings

AUT has not identified any information it holds that is of importance to Māori. However, AUT has produced a framework for engaging with Māori to design the process of identifying information of importance to Māori.

The Assistant Pro-Vice Chancellor (Māori Advancement) has an awareness of the information that may be of importance to Māori and will be involved in the formal identification and documentation of this information. There is a steering group made up of six Māori leaders across AUT who are currently consulting with Māori staff and students on this framework, which is related to the identification of information of importance to Māori. They will seek formal adoption of the framework by the AUT Council in July 2023.

Recommendation

Identify and document information of importance to Māori that is held by AUT.

Self-monitoring

Public offices are responsible for measuring and monitoring their information management performance for planning and improvement purposes. This helps to ensure that IM systems and processes are working effectively and efficiently. It also ensures that public offices are meeting the mandatory Information and records management standard as well as their own internal policies and processes.

TOPIC 7 – Self-monitoring — Progressing

Summary of findings

There is no regular, formal monitoring of compliance with information management requirements within AUT's departments. Issues around information management are discussed informally and as needed within departments. Staff interviewed noted they would

speak up if there was any evidence of non-compliance with any of the organisation's policies, including the Records Management Policy.

AUT completed an internal audit in June 2022 to assess information maturity against the IM Maturity Assessment. The recommendations of this are prioritised by timeframe. For example, an immediate action was to put in place key information management documents, such as the Information Management Strategy and an updated Records Management Policy. However, there is no monitoring programme for information management, and the Executive Sponsor's monitoring activities are informal in nature.

Recommendation

Refer to the recommendation for Topic 3 – *Governance arrangements and the Executive Sponsor.*

Capability

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

TOPIC 8 – Capacity and capability — Progressing

Summary of findings

AUT has no dedicated resource to perform the role of an information manager. Instead, AUT has engaged an external information management consultant to perform the function of an Information Manager. The Executive Sponsor's responsibilities are managed alongside other executive responsibilities, and the role is supported by the IM Consultant.

The Executive Sponsor noted through interviews that AUT's current information management capacity is lacking for the organisation's needs. In addition, information management capacity is not regularly monitored against business needs. Staff also noted that hiring additional resource was difficult due to the recent organisation-wide restructure.

The Executive Sponsor and IM Consultant have conducted some information management sessions for staff to improve awareness of AUT's Information Management Strategy, Policy and procedures. These sessions have not been conducted in all departments.

Staff complete information management training as required, such as system-specific training as part of induction. However, while staff have access to the Records Management Policy and Records Management Procedures via AUT's intranet, they do not have access to regular, mandatory information management training.

All staff interviewed were willing to improve information management practices across AUT. However, there was a recent organisation restructure, and as a result, AUT lacks a dedicated information management resource to drive this improvement work.

Recommendation

Regularly assess information management capacity and capability against business needs to ensure AUT is appropriately resourced.

TOPIC 9 – IM roles and responsibilities — Progressing

Summary of findings

Staff interviewed had a good awareness of information management responsibilities. This understanding was primarily developed through on-the-job training, for example for the payroll and human resources, and student administration systems. This training covers requirements such as where staff create this information, and that the information must be complete and accurate. Information management responsibilities are communicated to all staff via the Policy and Procedures documents.

In the sample of three position descriptions reviewed, all referenced the need to maintain accurate records. For example, one position description contained a general requirement to regularly review and update human resources information on the intranet. Another required AUT's personnel files and job evaluation information to be maintained to a high standard.

However, staff interviewed noted there is variability in the information management requirements in position descriptions and performance evaluations across AUT. Staff are required to comply with AUT policies, including the Records Management Policy.

Recommendation

Identify the training needs for information management and implement a training plan.

Creation

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

TOPIC 10 – Creation and capture of information — Progressing

Summary of findings

Staff and contractors are aware of their obligation to create and capture full and accurate records. The 'What to store where' guidelines explain where information can be appropriately created and stored. The guidelines also actively discourage staff from using uncontrolled environments. The Chief Technology Officer and CISO monitors the use of unapproved environments on an ad hoc basis as they become aware of their use, for example, use of USB drives and unapproved cloud storage, and instances of misuse are immediately addressed. However, staff noted that due to the size of the organisation it is difficult to monitor this across AUT.

Information is routinely created and captured as part of all business functions and activities. Recently developed document formatting and version control tables are used to promote reliability and trust in information. However, as referenced in Topic 7 – *Self-monitoring*, there is no structured approach to monitoring.

Recommendation

Formalise oversight and monitoring over uncontrolled environments to ensure staff keep information in controlled environments.

TOPIC 11 – High-value / high-risk information — Progressing

Summary of findings

Staff have an understanding of information assets which are of high-value or high-risk to AUT. The Director Data, Technology, Risk & Policy noted that AUT has started to create an information asset register which is being overseen by the DIGG. The draft register contains high- value or high-risk information such as student management data including credit and enrolment data, and states the source, retention period, and sensitivity classification of the information. The register has not been completed.

Additional protections and procedures are in place to safeguard information identified in the register. For example, limited access to the master data. In addition, there is an 'AUT Data and Information Sensitivity Classification' document summarising the risks, intended audiences and examples of five information classes. These classifications are used on the draft register.

Staff noted that AUT will continue to manage information based on the level of risk associated with it. The programme to develop this register has been designed to identify and mitigate data and information risks.

Recommendation

Complete the inventory of high-value/high-risk information assets in the information asset register.

Management

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

TOPIC 12 – IM requirements built into technology systems — Progressing

Summary of findings

Information management requirements are considered in the design and configuration decisions of some new and upgraded business systems. For instance, the recent implementation of a new service management system identified information management needs such as maintaining accurate and up-to-date information. In addition, audit logs can be used on SharePoint to track user activity through time-stamped document creation and modification data.

However, staff noted that considering information management requirements had not been a routine activity across all business systems and upgrades in the past, particularly with legacy systems. AUT require third-party solution providers to complete a survey to confirm that information, data, and cybersecurity policies are in place to protect AUT information. But the organisation lacks documented standardised information requirements to be considered when implementing or upgrading business systems.

There is an expectation that new and upgraded business systems meet minimum metadata requirements, but this may not always be possible where the system lacks the functionality to enable this. However, the new service management system does meet the minimum metadata requirements. During the decommissioning of systems, AUT expects system owners to communicate guidance on what happens with the information decommissioned systems contain, but does not document this expectation. As a result, there is an inconsistent approach to information management during these changes.

Recommendation

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

TOPIC 13 – Integrity of information — Progressing

Summary of findings

There are localised information management practices at AUT. There is no consistent approach to information management "good practice" across AUT and the approach is highly dependent on individual departments. As a result, information is not managed consistently across AUT.

However, AUT is developing its organisation-wide information management practices. As referenced in Topic 10 – *Creation and capture of information,* ICT has recently published 'What to store where' guidelines on the intranet. These guidelines promote good practice by explaining where information should be created, used, and accessed depending on their intended use, audience and sensitivity classification. In addition, while there are localised approaches to naming conventions, AUT has developed a consistent approach to formatting and version control for policy and procedure documents which supports the integrity of information in these documents.

Staff and contractors have variable experiences when trying to find and retrieve information. For example, staff noted during focus groups that it can be difficult to find information created by another department. A new search function is available through the intranet to enable an entire Microsoft 365 suit search. However, it is acknowledged that not all information should be accessible to everyone in the organisation. While at the time of the audit this was still being tested, the Director Data, Technology, Risk & Policy noted that it should greatly improve AUT's enterprise-wide search capabilities.

Recommendation

Identify and address user experience issues with finding and retrieving information.

TOPIC 14 – Information maintenance and accessibility — Progressing

Summary of findings

There are strategies in place to manage and maintain digital information during some business and system change projects. For example, during payroll and human resources system changes there was testing prior to and after migration and constant monitoring by the IT team to assign and track role-based permissions.

Some risks to accessing physical information have been identified. AUT has conducted ad hoc digitisation projects in the past, for example, of staff files in the People and Culture team. However, there are no formal documented strategies to manage and maintain physical information during business and system changes.

Preservation and continuity needs for digital information are identified, and plans are in place to address these. All systems have processes to ensure data is protected and preserved. AUT has a list of applications at risk of becoming obsolete and has identified strategies to mitigate preservation and accessibility risks.

Recommendation

Establish a periodic review of ongoing accessibility risks and preservation needs for physical and digital information.

TOPIC 15 – Business continuity and recovery — Progressing

Summary of findings

AUT has a business continuity plan (BCP) called the 'AUT Business Continuity and Disaster Recovery Plan' which was last updated in May 2022. A critical processes document, 'Critical Processes – Business, Economics and Law' supports the BCP, but applies only to the Faculty of Business and Law.

The AUT BCP focuses on ICT and outlines disaster recovery failover processes, and procedures for technology recovery activities. It includes potential scenarios, their impact, actions required to remedy the issues, and responsibilities. For example, it outlines a process for Core Data Centre LAN switch failure and the backup process used to restore access to digital information. This is where various network devices, such as servers and storage systems, stop communicating with each other. The BCP is regularly tested, the most recent test being completed in September 2022.

The Critical Processes – Business, Economics and Law document provides guidance on workarounds for the loss of facilities (including building, equipment and physical information), people and IT across four core processes – teaching, assessment, examinations and student administration. While it identifies critical information in these four processes, it applies only to the Faculty of Business and Law. Additionally, there is no documented plan for accessing physical information in event of a business disruption.

Recommendation

Ensure the BCP identifies critical information for all departments.

Storage

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

TOPIC 16 – Appropriate storage arrangements — Progressing

Summary of findings

AUT has protection and security controls in place for some physical information held internally. For example, physical copies of student records held in the Student Administration building are secured by swipe access, with access limited to approved personnel. Files were labelled by year and protected against hazards such as fire with a sprinkler system installed. AUT also store historical information with a third-party provider.

AUT has protection and security controls in place for digital information. Digital information is largely stored in SharePoint, with additional information saved to relevant systems such as the student management system. Access to data in SharePoint requires two-factor authentication and is restricted to permissions set by IT staff or the folder owner. For example, the personal information of staff can only be accessed by select members of the People and Culture team.

There is currently no regular reporting of information protection and security risks to the Executive Sponsor. Without regular reporting, the Executive Team and DIGG cannot effectively support the remediation of any of AUT's information protection and security risks.

Recommendation

Identify information protection and security risks and regularly report these to the Executive Sponsor and DIGG.

Access

Ongoing access to and use of information enables staff to do their work and the public to hold government accountable. To facilitate this, public offices need mechanisms for finding and using this information efficiently. Information and/or data sharing between public offices and with external organisations should be documented in specific information sharing agreements.

TOPIC 18 – Information access, use and sharing — Progressing

Summary of findings

Staff understand how to use AUT's business and information systems as this is covered during their onboarding or ongoing on-the-job training. AUT takes a decentralised approach to information management where each department is responsible for maintaining the information it creates and uses.

However, as referenced in Topic 10 – *Creation and capture of information* the 'What to store where' guidelines published on AUT's intranet explain where staff can appropriately collaborate and share information across a range of classifications, information descriptions, risk categories, and audiences. Additionally, they provide guidance on how to use OneDrive, Teams, SharePoint, cloud storage providers, and Home Drives. They apply to all staff and file storage except research data.

Staff interviewed knew how to use systems and understood when their roles required them to create, control and facilitate access to information. If they identified information management issues, staff understood that individual departments are responsible for information management, but that guidance could be obtained from the IM Consultant, Director Data, Technology, Risk & Policy and members of the DIGG.

Information is controlled by restricted access to AUT's business and information systems. Access controls for AUT's core digital systems are well understood by system owners. However, the level of documentation around access controls for AUT's systems varies. For example, there is a document outlining the permissions for the release of information from the AUT Data Warehouse for business intelligence reporting. Similar documentation does not exist for all core business systems.

Physical copies of student records in the Student Administration building have restricted access, which is controlled by the Records, Compliance and Graduation Manager. Staff must be accompanied by the Records, Compliance and Graduation Manager or one of the three members of the Records, Compliance and Graduation team.

As referenced in Topic 13 – *Integrity of Information* staff noted that they sometimes have difficulty retrieving documents outside of their departments. Some systems comply with minimum metadata requirements, such as SharePoint. However, staff noted that AUT plans on using metadata labelling across all key systems to enable better capabilities, such as automated actions and protections to be applied to digital information.

Recommendations

Document user access controls for core business and information systems in a consistent manner. Regularly monitor access controls and ensure they are appropriately applied.

Ensure all information is created and captured on appropriate systems that meet the minimum metadata of Te Rua Mahara requirements where possible.

Disposal

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

TOPIC 20 – Current organisation-specific disposal authorities — Managing

Summary of findings

AUT is part of a Disposal Authority (DA702) that applies to eight New Zealand universities. It was authorised in 2021 and the next review is scheduled for 2031. The disposal authority covers all information formats, faculties and service divisions. AUT is also covered by the General Disposal Authorities (GDA) 6 and 7.

AUT does not have a regular review cycle to ensure that the disposal authority reflects business and legislative changes. If any revisions to the disposal authority were deemed to be necessary, the Executive Sponsor and IM Consultant would raise it with other Records Managers at the New Zealand Universities Records Management forum.

While staff and contractors have a general awareness of their responsibilities regarding disposal of information, there is currently no training provided to staff.

Recommendation

Provide guidance to staff on disposal requirements relevant to the types of information they manage.

TOPIC 21 – Implementation of disposal decisions — Beginning

Summary of findings

AUT has approval to dispose of information under DA702 and GDA 6 and 7. One instance of disposal has been documented and staff interviewed were not aware of any other documented instances of disposals. As information could be stored in uncontrolled environments, information may have been disposed of without being documented.

The People and Culture team developed a process in September 2019 to dispose of active and recently terminated permanent and fixed-term employee information after it had been digitised. A disposal decision was implemented in accordance with this policy in December 2019. It was well documented and approved by the relevant business owner and sponsor, and ultimately, the Executive Sponsor.

There are no formal plans to dispose of physical or digital information, and no organisation-wide processes are currently in place to identify information that can be disposed of under the organisation-specific disposal authority. This will result in AUT retaining information for longer than required.

Recommendation

Develop an implementation plan to dispose of physical and digital information under the relevant disposal authorities.

TOPIC 22 – Transfer to Te Rua Mahara — Beginning

Summary of findings

There have been no information transfers to Te Rua Mahara in either physical or digital formats. As AUT was established in 2000, there is no information created or captured by AUT that is older than 25 years. However, AUT maintains information of predecessor institutions which are older than 25 years. It has not identified physical and digital information of archival value that is over 25 years old or determined whether such information is open or restricted access.

Recommendation

Identify physical information of archival value that is older than 25 years and start to prepare this information for transfer to the Te Rua Mahara office in Auckland.

6. Summary of feedback

Auckland University of Technology, Te Wananga Aronui o Tamaki Makau Rau, thanks the auditors for their constructive approach to the audit engagement and accurate recording of the information management practices across the organisation.

The audit provides the University with clear direction and areas of future focus to continue its improvement of information management maturity and practices. The University welcomes the recommendations. These will be reviewed and reflected as actions and outcomes in the organisation's existing information management strategy.

It is noted that as far as practicable, recommendations will be implemented using existing resources. Due to the ongoing financial challenges faced by the tertiary sector, including the University, there may however be limitations on or delays to the progression of some recommendations if additional resourcing or budget is required.

7. Appendix 1

The table in Section 4, on page 3 lists all assessed maturity levels by topic area in a table format. This table has been listed below for accessibility purposes:

Topic 1, IM strategy – Maturing

Topic 2, IM policy and processes – Managing

Topic 3, Governance arrangements & Executive Sponsor – Managing

Topic 4, IM integration into business processes – Progressing

Topic 5, Outsourced functions and collaborative arrangements – Progressing

Topic 6, Te Tiriti o Waitangi – Beginning

Topic 7, Self-monitoring – Progressing

Topic 8, Capability and capacity – Progressing

Topic 9, IM roles and responsibilities – Progressing

Topic 10, Creation and capture of information – Progressing

Topic 11, High-value / high-risk information – Progressing

Topic 12, IM requirements built into technology systems – Progressing

Topic 13, Integrity of information – Progressing

Topic 14, Information maintenance and accessibility – Progressing

Topic 15, Business continuity and recovery – Progressing

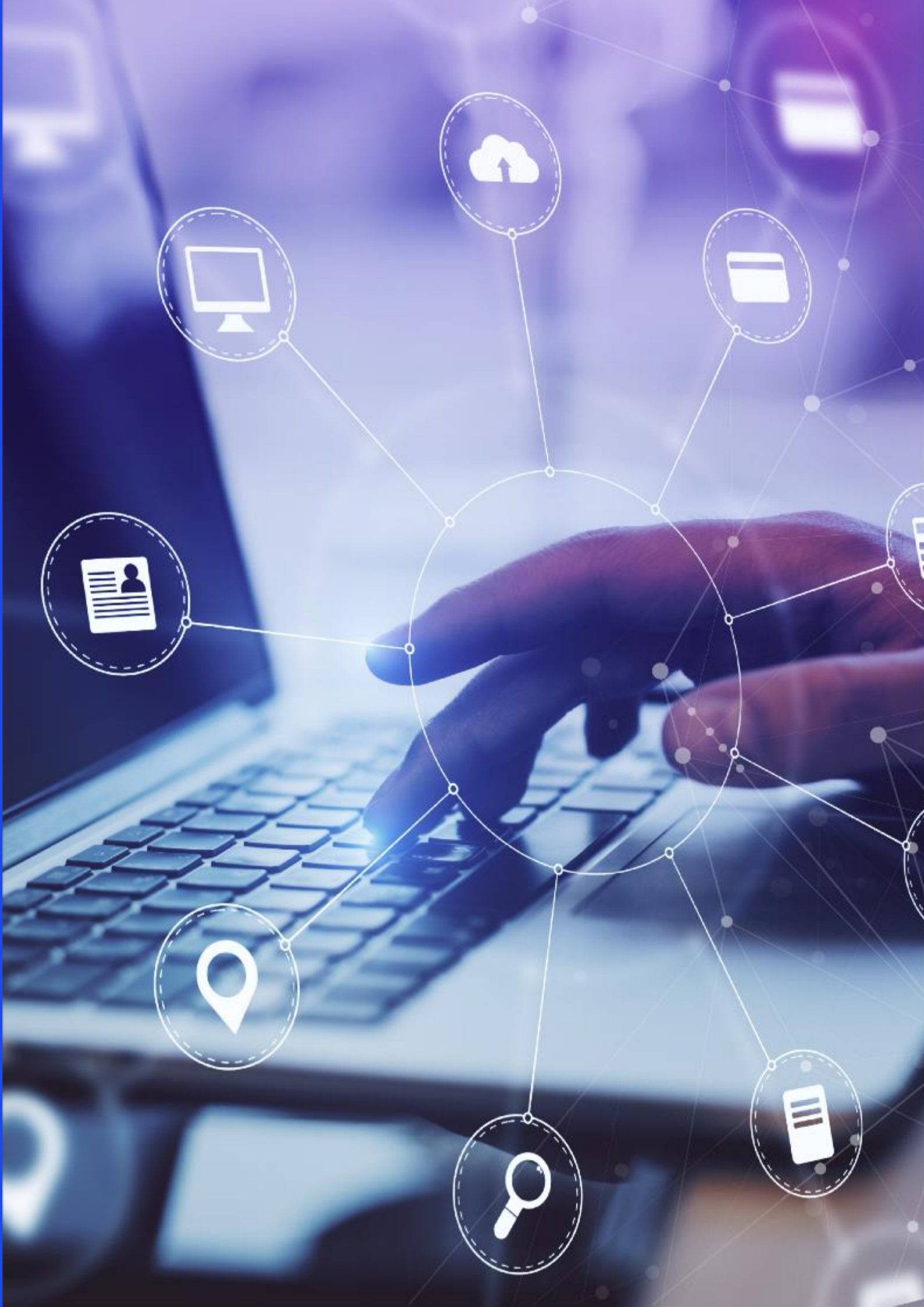
Topic 16, Appropriate storage arrangements – Progressing

Topic 18, Information access, use and sharing – Progressing

Topic 20, Current organisation-specific disposal authorities – Managing

Topic 21, Implementation of disposal decisions – Beginning

Topic 22, Transfer to Te Rua Mahara – Beginning



Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND

9 February 2024

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

Damon Salesa
Vice-Chancellor
Auckland University of Technology
damon.salesa@aut.ac.nz

E te rangatira e Damon, tēnā koe

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the Auckland University of Technology (AUT) completed by KPMG under section 33 of the Public Records Act 2005 (PRA). Thank you for making your staff and resources available to support the audit process.

Introduction

Te Rua Mahara o te Kāwanatanga Archives New Zealand (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 the mandatory Information and records management standard. AUT has been assessed as having IM maturity mostly operating at the 'Progressing' level.

For business owners, good awareness of their IM role and responsibilities means that they can support their staff. Even with a distributed operational model there must be appropriate specialist oversight for IM to operate effectively. For an organisation of 2249 full time staff, the IM capacity is low. This affects the ability to support business owners, provide IM induction and control and monitor IM across the organisation to improve IM consistency.

There has been useful work done to develop the Information Management Strategy and Roadmap and the Records Management Policy and Procedures. Further work is needed from the organisation to embed improvement and support staff who are aware of their IM obligations but lack enough dedicated specialist resource.

Prioritised recommendations

The audit report lists 22 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 nine 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 iti noa, nā

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

Cc Andrea Vujnovich, Assistant Vice-Chancellor, Corporate and General Counsel (Executive Sponsor), andrea.vujnovich@aut.ac.nz

APPENDIX

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Governance	4: IM integration into business processes	*Provide information management training to business owners to increase their understanding of information management responsibilities.*	With a decentralised IM system, business owners need to have a good understanding of their IM role and responsibilities so that they can disseminate and support good IM practice in their business unit. This needs to be done with the support of a specialist IM resource.
Governance	6: Te Tiriti o Waitangi	*Identify and document information of importance to Māori that is held by AUT.*	This is an area of work that could benefit from collaboration with other universities using the New Zealand Universities Records Management forum.
Self-monitoring	7: Self-monitoring	*Decide what information management activity needs regular monitoring. Implement a plan to report on it to DIGG via the Executive Sponsor. (Same recommendation as for Topic 3: Governance arrangements and Executive Sponsor).*	This will provide information on key IM activities to ensure trends are identified and issues raised. This could include formalising and monitoring uncontrolled environments (recommendation for Topic 10: Creation and capture of information).
Capability	8: Capacity and capability	*Regularly assess information management capacity and capability against business needs to ensure AUT is appropriately resourced.*	A successful decentralised system needs to be supported with good documentation and specialist oversight including staff training. This can be provided internally or externally but needs to be enough to ensure appropriate support and development.
Capability	9: IM roles and responsibilities	*Identify the training needs for information management and implement a training plan.*	It is useful if IM induction training is mandatory for all new starters and that regular refresher training is provided as the need is identified.

Category	Topic Number	Auditor's Recommendation	Comments from Te Rua Mahara
Management	11: High-value/high-risk	*Complete the inventory of high-value/high-risk information assets in the information asset register.*	This can be done with reference to the appraisal work done for DA702 and will help AUT to prioritise work with its information. Sharing this with others in the sector could help in deciding consistent asset groups across the sector.
Management	13: Integrity of information	*Identify and address user experience issues with finding and retrieving information.*	Understanding the pain points in use of the systems is the first step in ensuring that systems are fit for purpose and assist staff in their daily work.
Disposal	21: Implementation of disposal decisions	*Develop an implementation plan to dispose of physical and digital information under the relevant disposal authorities.*	AUT should take advantage of the disposal authority and develop a plan for implementing disposal including transfer. This could be discussed at the New Zealand Universities Records Management forum and a plan developed collaboratively if possible.
Disposal	22: Transfer to Te Rua Mahara	*Identify physical information that is older than 25 years and start to prepare this information for transfer to the Te Rua Mahara Auckland office.*	This information is from predecessor organisations and the experience will enable AUT to continue with its own information when reaching 25 years of age.