Deloitte.

Kordia Group Limited
Public Records Act 2005 Audit Report

Prepared for Archives New Zealand

December 2021

MAKING AN IMPACT THAT MATTERS since 1845

Table of Contents

1. Disclaimers 2
2. Executive Summary 3
3. Introduction 4
4. Information Management Maturity Summary 5
5. Audit Findings by Category and Topic 6
    - Governance 6
    - Capability 10
    - Creation 11
    - Management 12
    - Storage 14
    - Access 15
    - Disposal 16
6. Summary of Feedback 17

1. Disclaimers

Use of Report

This report was prepared for the use of Archives New Zealand (Archives NZ) and Kordia Group Limited. It was prepared at the direction of Archives NZ 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 NZ in accordance with the independence requirements of the Public Records Act 2005 (PRA). We also adhere to the independence requirements of Professional and Ethical Standard 1 (Revised): Code of Ethics for Assurance Practitioners issued by the New Zealand Auditing and Assurance Standards Board. Other than this audit programme, we have no relationship with or interests in Archives NZ.

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 Kordia Group Limited and Archives NZ who 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 Archives NZ's 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 Kordia Group Limited and Archives NZ. 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 NZ. These procedures are designed to identify control weaknesses but cannot be relied upon to identify all weaknesses.

2. Executive Summary

Kordia Group Limited

Kordia Group Limited (Kordia) is a state-owned enterprise, established in 2004 as Transmission Holdings Limited under the Television New Zealand (Separation of Transmission Business) Order 2003 and the Television New Zealand Act 2003. It was renamed to Kordia Group in 2006. Kordia is a telecommunications, cybersecurity and media business that provides network and technology solutions. It is governed by State-owned Enterprises Act

Kordia has approximately 10 employees primarily in Auckland, New Zealand. Kordia has three subsidiaries Kordia New Zealand Limited and its subsidiary Kordia Limited (Kordia NZ); and Kordia Pty Limited (Australia). These subsidiaries are not in scope of this review, as they do not come under the PRA. As Kordia is a small organisation, Kordia NZ provides a large portion of its operational services.

The high-value / high-risk records that Kordia holds include board papers, financial records, and employee's personal information.

Within the last 12 months a change programme has begun to uplift the state of information management (IM). This work programme has included hiring an IM contractor to complete an IM health check, develop a strategy and IM policy. There are currently no dedicated IM staff with no confirmed plans to employ ~~an~~ IM staff, however, several employees support the IM programme in conjunction with their main responsibilities.

Summary of Findings

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

Maturity Level	Beginning	Progressing	Managing	Maturing	Optimising
No. of Findings	4	6	7	3	–

3. Introduction

Background

Archives NZ provides IM leadership across the New Zealand 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;
- the government is open, transparent and accountable by making public sector IM practices known to the public.

Section 33 of the (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 NZ's monitoring of 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 for certain public offices.

Objective

The objective of these audits is 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. They 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 Kordia's IM practices against Archives NZ's IM Maturity Assessment model. The IM Maturity Assessment aligns with the PRA and Archives NZ's mandatory Information and Records Management standard. Topics 17 and 19 of the Archives NZ 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). Kordia's maturity level for each topic area is highlighted under each of the respective areas. Ratings were based on Kordia's officials' responses to questions during the interviews and the supporting documents provided in line with the IM Maturity Assessment guidelines.

Archives NZ 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 NZ reviewed before release to Kordia. Archives NZ is responsible for following up on the report's recommendations with Kordia.

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.

Kordia'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.

Category	No.	Topic	Assessed Maturity Level				
			Beginning	Progressing	Managing	Maturing	Optimising
Governance	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	7	Self-monitoring		●			
Capability	8	Capacity and Capability		●			
	9	IM Roles and Responsibilities		●			
Creation	10	Creation and capture of information			●		
	11	High-value / high-risk information			●		
Management	12	IM requirements built into technology systems			●		
	13	Integrity of information			●		
	14	Information maintenance and accessibility		●			
	15	Business continuity and recovery				●	
Storage	16	Appropriate storage arrangements				●	
Access	18	Information access, use and sharing		●			
Disposal	20	Current organisation-specific disposal authorities	●				
	21	Implementation of disposal decisions	●				
	22	Transfer to Archives New Zealand	●				

Note: Topics 17 and 19 of the Archives NZ 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.

Managing

Observations

Kordia has a current IM Strategy, which senior management approved in September 2021. The IM Strategy is a three-year plan (2021-2024) with two key strategic initiatives and underpinning IM principles. The strategic initiatives are to improve Kordia's compliance with external IM requirements and optimise IM across Kordia NZ. While we did not identify any areas of divergence from Kordia's broader strategic direction, the strategy does not explicitly align with the strategic direction or the wider sector direction, as neither are mentioned in the strategy.

The IM strategy includes a roadmap of how Kordia (NZ and Group) will achieve its strategic goals and is available on Kordia's intranet. This roadmap includes key activities and initiates to improve Kordia's overall IM maturity. Key dependencies to achieve initiatives are also identified in the roadmap, which includes a new IM specialist role. There is no regular reporting of progress towards the strategy initiatives.

Recommendations

1. Prioritise addressing key strategic dependencies. For example, resourcing an IM specialist role across Kordia NZ and Group.

2. Introduce regular status reporting on the identified IM strategic initiatives.

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

Kordia has an IM Policy, which includes documented roles and responsibilities, and process documentation per category of information. Senior management approved the IM Policy, which was last updated in May 2021. It is consistent with the IM Strategy and links to other policies such as Information Security. The IM Policy is also available on Kordia's' intranet along with the IM Strategy.

Compliance with the Policy is not actively monitored and is addressed in an ad hoc manner.

Recommendation

1. Proactively monitor the IM policy and report on any policy breaches to the IM governance group.

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.

Maturing

Observations

Kordia has two governance groups, the Security Governance Group (SGG) and the Security Management Group (SMG), whose attendees include the Executive Sponsor, the Chief Information Security Officer, and several other members of senior management. Both groups cover aspects of IM. SGG provides governance oversight of Kordia's Security Programme, which includes IM, along with information security, physical security, privacy, and business continuity. SMG supports SGG and provides management oversight of the Security Programme. The groups meet quarterly and are formalised with a Terms of Reference, recorded meeting minutes and regular reporting.

The Executive Sponsor understands and consistently performs the oversight and monitoring role relating to IM. They support IM within Kordia Group and Kordia NZ, through promoting the value of IM at a senior management level. Within the last twelve months this has led to the performance of an IM health check and developing the IM Strategy and Policy.

Recommendation

1. The Executive Sponsor to work with other Executive Sponsors outside of Kordia for guidance and support to continue IM strategic improvements.

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.

Managing

Observations

Due to the small size of Kordia and the type of work performed, IM is integrated into everyday processes and recognised by business owners. Financial information follows specific, documented processes within the finance system. Board papers are consistently created, filed, and protected, and stored within Diligent. Specific roles and responsibilities are outlined in the IM Policy, which all business owners are aware of. Office 365, which includes SharePoint is also actively used within Kordia Group, with consistent creation and use of information processes. Shared drives are still available to store information that isn't within Diligent, or the finance system, however Office 365 is the primary system.

Kordia does not have a specific IM team, however, staff with IM expertise within Kordia NZ provide support to the Group. Any IM issues would be raised to the appropriate staff member or escalated to SGG if necessary.

Kordia has not had any recent business change. However, Kordia NZ has a Design Procedure, which covers IM, and would apply to the Group in the instance of a business change.

Recommendation

1. Introduce IM as a measure within performance plans to ensure business owners are actively fulfilling their responsibilities and are monitored.

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

Kordia service contracts with outsourced IT services refer to confidentiality, data ownership, maintaining records and intellectual property. However, there is no regular monitoring over the contracts in place to ensure compliance with the PRA.

Kordia does not have any collaborative arrangements.

Recommendation

1. Ensure relevant IM requirements are included in all contracts where public records are created and develop a regular monitoring process to ensure suppliers are compliant with IM requirements under the PRA.

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.

Beginning

Observations

Kordia has an information asset register (IAR), which includes a category evaluating both the value/significance of the information asset, and loss, to New Zealand. However, it does not specify if information has been assessed as significant to Māori, or apply to Te Tiriti o Waitangi. Outside of the IAR, implications of the Te Tiriti o Waitangi principles on IM processes are not known.

Recommendation

1. Identify information of importance to Māori within IAR.

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

There is no formalised monitoring of compliance with the PRA. Regular reporting to the Security Governance Group and Information Security Management Group does not specifically focus on the PRA or IM Policy. Non-compliance is reported on an ad hoc basis to the Security Governance Group, with avenues for further escalation to broader senior management if the non-compliance is significant.

A contracted IM specialist completed an IM Health Check in April 2021. This assessed Kordia's current state and resulted in key findings and actions. These recommendations informed the creation of the IM Strategy and roadmap and IM Policy.

Recommendation

1. Develop a monitoring process that covers compliance with the IM Policy, the PRA and other requirements and report results to the Executive Sponsor and the Security Governance Group.

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

Kordia's current IM team, serviced through Kordia NZ, consists of the Chief Information Security Officer and an Application Manager. Both have full time commitments across Kordia NZ, outside of IM. The IM team have appropriate skills, although lack capacity to provide sufficient IM support to the Group and Kordia NZ.

A contractor has been brought in, as mentioned above, to complete a health check and provide IM support. This contractor is available on an on-going basis when IM expertise are required. The Executive Sponsor acknowledged the lack of capacity and reported plans to recruit for a full time IM staff, although this is dependent on approval in the next quarter budget.

The IM team reported sufficient access to IM professional development through both internal and external courses.

Recommendation

1. Determine the current gaps in IM staff capacity. Once requirements are determined, develop a business case to gain approval in the next budget review to address IM requirements.

Topic 9: IM Roles and Responsibilities

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

Progressing

Observations

IM responsibilities are specifically outlined in the Code of Conduct. Staff interviewed are aware of their individual obligations within their roles, and of the IM Strategy and Policy. IM responsibilities are outlined in the Information Asset Owner role descriptions; however, it is unclear how many staff this IM description applies to.

There is no IM specific induction training and there has been no recent IM training. Main training provided for staff is on-the-job and the informal induction training from fellow staff members. Despite a lack of formal training, there is a detailed IM Guide available to all staff on the intranet, with a decision-making flowchart to support appropriate IM processes.

Recommendation

1. Identify IM training needs of staff and contractors and deliver through appropriate communication to meet this need.

Creation

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

Topic 10: Creation and Capture of Information

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

Managing

Observations

Staff understand their responsibility to create full and accurate information to support business functions and to formally document Kordia's activities. Kordia's corporate functions include creating board papers and financial information, and within these functions there is a strong staff awareness of IM best practice. Kordia also has a Disaster Recovery Plan and Backup policy, these demonstrate understanding of the importance of maintaining full and accurate records.

Kordia uses SharePoint on-premise, but are transitioning to Office 365 as their primary system. Due to access controls, there is a high level of confidence that information is managed in a controlled environment. Appropriate metadata requirements are built into both SharePoint on-premise and Office 365. Shared drives are still available for use, however access controls per business unit, restrict the ability for inappropriate capture of information.

All staff reported confidence in the reliability and integrity of information. As Kordia is a small organisation with only 10 employees, there are clear structured approaches to IM within each business unit, with any variances quickly identified and mitigated.

All new information is created digitally.

Recommendation

1. Discourage the use of or decommission systems that do not meet metadata requirements, for example shared drives.

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.

Managing

Observations

The IM team has created an IAR to capture information, including information classified as high-value/high-risk. The IAR assesses value and risk using criteria such as, the value to Kordia, the broader sector and value to New Zealand, as well as the impact to all three if the information was lost. The IAR also records information containing personal details and security classifications. IAR also references the applicable General Disposal Authority if relevant per information asset.

Although there is thorough categorisation there is limited analysis of risks per information asset.

The current IAR also lacks any date of completion, or process to update, therefore is difficult to determine if it is up to date.

Recommendations

1. Include a date completed reference, and next review date in IAR, to ensure it is both current and is regularly updated.

2. Add a category within the IAR to identify any risks per information asset, and any controls in place to mitigate this risk.

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.

Managing

Observations

Kordia seeks IM expertise and advice when implementing and upgrading technology systems. Commissioning and decommissioning of any systems -is subject to an approval process, which Kordia NZ oversees and manages. This process would apply to Kordia in the instance of a relevant system change. As the current IM team includes the Chief Information Security Officer, any technology solutions are already approved by an IM team member.

Kordia and Kordia NZ have a Design Procedure, which outlines the roles, responsibilities, documentation requirements and approval process for any cyber developments.

The recent migration from SharePoint on-premise to Office 365 for both Kordia and Kordia NZ included IM requirements in the migration. This included verifying the integrity of information throughout migration. Metadata requirements were already met through SharePoint on-premise.

Office 365 has an automatic retention policy of ten years, Kordia also has a backup and retention policy. However, retention of backups does not meet IM standards for retention. Also, risks of systems that do not meet metadata requirements are not actively identified, for example shared drives.

Recommendation

1. Formally identify the risks of any system which do not meet metadata, or IM retention requirements and introduce appropriate control and mitigation strategies.

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.

Managing

Observations

Staff reported a high level of confidence in the reliability, findability and trustworthiness of information created and captured within Kordia systems. There is variation of IM processes between business units, such as Finance and the Governance team, however this is due to the different nature of the information and systems. There is a separate system for payroll and board papers.

In addition to the policy and strategy, IM guidance is available on the intranet, however there is limited active monitoring of the integrity of information by the IM team.

Recommendation

1. Gain approval in the budget review to recruit / contract more IM capacity, to increase active monitoring of IM processes and ability to provide training to staff.

Topic 14: Information Maintenance and Accessibility

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

Progressing

Observations

A clear strategy to manage and maintain physical or digital information during business and system changes is not in place. However, the Information Classification Policy outlines the lifecycle of information per classification, which indirectly covers maintenance and accessibility over time.

Additionally, general accessibility of physical information is ensured through long-term ongoing storage of information with an off-site commercial provider. Kordia retains an index of all stored information and can request it back at any time.

Digital information also remains accessible and maintained overtime, through access control, format, and metadata continuity. Security processes and continuous updates of systems ensure digital information is still accessible over time. Long term preservation of digital continuity is not formalised in a strategy, though staff reported a conscious effort and awareness of maintaining accessibility.

Recommendation

1. Formally identify digital continuity needs for digital information to inform IM work programme planning.

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.

Maturing

Observations

Kordia Group has a Disaster Recovery Plan which outlines the response for any technology disaster recovery. Included within this plan is a list of critical systems, prioritisation of these systems, notification tree, and contact information. The plan is set to be tested every 24 months. Although the plan is thorough, it does not reference the recovery of any physical information.

Kordia also has a Data Breach Response Plan which was last updated November 2020. This plan outlines the steps Kordia would take in the instance of a data breach, specifically related to any personal information it holds. Members of the response team are clearly identified, with roles and responsibilities defined. The plan relates specifically to the Privacy Act.

Internal systems are regularly backed up with comprehensive access controls in place. Backups are taken daily, weekly, monthly, and annually and there is regular testing of digital system backups to ensure information can be restored. Backups and retentions standards are outlined in Kordia Group's Information Security Backup Policy. Included within this policy is the governance structure over backups and maintenance plans for specific systems.

Recommendation

1. Add a section within the Disaster Recovery Plan which outlines the response, responsibility, and prioritisation for physical information.

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.

Maturing

Observations

A large portion of Kordia's physical information is kept with a third-party storage provider.

Physical information kept onsite is stored in lockable cabinets and is labelled ensuring it remains accessible. This includes high-risk information such as financial and personal records. Only the Finance and Human Resources team have access to these cabinets. It is stored in an office-environment, which includes fire safety, flood mitigation and access control.

Digital information storage is managed through third-party providers, for example Microsoft through Kordia NZ. All digital information has restricted access to the appropriate roles, and legal hold prevents any deletion from emails. All on-premise digital environments are stored at the production centre in Hamilton. Whereas, Office 365 data is stored in Sydney, Australia at the Microsoft Data Centre.

Requirements for information security and protection are built-in to the respective service contracts through Kordia NZ. There are regular backups taken of all digital systems. Any security incidents are report to SGG. Audit logs are available for each system to check for unauthorised access, however this is not regularly monitored.

Recommendation

1. Ensure information protection and security risks are regularly reported to the IM governance group, and remediation actions are identified and monitored.

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

All staff reported the information they required for their work is findable, accessible, and consistently managed. There are consistent naming conventions and no reported version control issues. Metadata requirements are met through Office 365, however not all information is on this system resulting in inconsistent metadata across Kordia.

Kordia does not have any information sharing arrangements with other organisations. Kordia applies access controls for both physical and digital information. Access controls are in place across all digital systems, including restricting access to folders within shared drives or access to whole systems. Requesting access permission is a rigorous process through the IT service desk, which is administered by Kordia NZ.

Recommendation

1. Plan to decommission systems that do not meet metadata requirement.

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 NZ (or have a deferral of transfer) and be

Topic 20: Current Organisation-Specific Disposal Authorities

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

Beginning

Observations

Kordia does not have a current specific Disposal Authority (DA).

Recommendation

1. Develop and gain approval for a Kordia specific 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.

Beginning

Observations

Kordia does not have a current organisation-specific DA, therefore no information has been disposed of under a Kordia specific DA. There is an automatic ten-year hold on digital information, and a culture of retaining information. Subsequently there have been no reported instances of disposal under the GDAs.

Recommendations

1. Once a specific DA has been developed, identify what, if any, information may be disposed of under the DA or GDAs. Once this information is identified, create and complete a formalised disposal process.

2. Introduce training of disposal requirements to improve the culture of retention.

Topic 22: Transfer to Archives New Zealand

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

Beginning

Observations

Kordia has not identified or transferred, information that is older than twenty-five years or of archival value.

Recommendation

1. When Kordia has developed their organisation-specific disposal authority the information of archival value can be determined and transferred when appropriate.

6. Summary of Feedback

This section sets out Kordia's feedback pursuant to this PRA audit.

Kordia appreciates the constructive engagement of the audit team and the feedback in this report. Kordia considers the assessments to be balanced and has no issue with the maturity assessments made. Kordia recognises it has work to do to mature its systems and processes to the level it desires to operate at. The recommendations made in this report will be helpful in prioritising and pursuing the necessary improvements.

Deloitte.

Te Rua Mahara o te Kāwanatanga
ARCHIVES NEW ZEALAND

4 March 2022

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

Shaun Rendell
Chief Executive
Kordia Group Limited
Shaun.rendell@kordia.co.nz

Tēnā koe Shaun

Public Records Act 2005 Audit Recommendations

This letter contains my recommendations related to the recent independent audit of the Kordia Group Limited 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

Archives New Zealand (Archives) is mandated by the PRA to regulate public sector information management (IM). The audit programme is a key regulatory tool in our Monitoring Framework.

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

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

Audit findings

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

Organisations that are assessed as having a maturity level of 'Managing' across all IM topics are broadly meeting the minimum requirements expected by the PRA and Archives' mandatory Information and records management standard.

Kordia has maturity levels ranging from 'Beginning' to 'Maturing'. The new IM Strategy shows commitment to IM improvement and includes a new IM specialist role which is essential in supporting the activities and initiatives in the roadmap.

Prioritised recommendations

The audit report lists 23 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 six recommendations as identified in the Appendix.

What will happen next

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

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

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

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

Nāku noa, nā

Antony Moss
Acting Chief Archivist Kaipupuri Matua
Archives New Zealand Te Rua Mahara o te Kāwanatanga

Cc Michael Jamieson, Executive General Manager, Legal and Risk
Michael.jamieson@kordia.co.nz (Executive Sponsor)

APPENDIX

Category	Topic Number	Auditor's Recommendation	Archives New Zealand's Comments
Self-Monitoring	7: Self-Monitoring	*Develop a monitoring process that covers compliance with the IM Policy, the PRA and other requirements and report results to the Executive Sponsor and the Security Governance Group.*	Regular reporting ensures control over the IM systems and processes.
Capability	8: Capacity and Capability	*Determine the current gaps in IM staff capacity. Once requirements are determined, develop a business case to gain approval in the next budget review to address IM requirements.*	It is essential to have the right level of IM support both capacity and capability. This would also support the recommendation for Topic 9: *Roles and Responsibilities*.
Creation	11: High-Value/High-Risk Information	*Include a date completed reference, and next review date in IAR, to ensure it is both current and is regularly updated.*	A lot of good work has been done to create the IAR and updating will ensure it continues to be fit for purpose and aligns with the organisation's disposal authority.
Management	14: Information Maintenance and Accessibility	*Formally identify digital continuity needs for digital information to inform IM work programme planning.*	This can be integrated with the IAR to ensure that high-value/high-risk digital information is well managed.
Access	18: Information Access, Use and Sharing	*Plan to decommission systems that do not meet metadata requirement.*	For a small organisation it would be sensible to concentrate information in systems designed to meet metadata requirements. Additionally, multiple environments all need to be monitored and maintained.
Disposal	20: Current Organisation-Specific Disposal Authorities	*Develop and gain approval for a Kordia specific DA.*	This is the basis for other improvement in the disposal area. The IAE can be used to develop the disposal authority.