KPMG

# Data Protection and Privacy

## Internal Audit Report

**The Corporation of the City of Adelaide (CoA)**

—

May 2024

# Acknowledgement of Country

**KPMG acknowledges Aboriginal and Torres Strait Islander peoples as the First Peoples of Australia. We pay our respects to Elders past, present, and future as the Traditional Custodians of the land, water and skies of where we work.**

At KPMG, our future is one where all Australians are united by a shared, honest, and complete understanding of our past, present, and future. We are committed to making this future a reality. Our story celebrates and acknowledges that the cultures, histories, rights, and voices of Aboriginal and Torres Strait Islander People are heard, understood, respected, and celebrated.

Australia's First Peoples continue to hold distinctive cultural, spiritual, physical and economical relationships with their land, water and skies. We take our obligations to the land and environments in which we operate seriously.

Guided by our purpose to 'Inspire Confidence. Empower Change', we are committed to placing truth-telling, self-determination and cultural safety at the centre of our approach. Driven by our commitment to achieving this, KPMG has implemented mandatory cultural awareness training for all staff as well as our Indigenous Peoples Policy. This sincere and sustained commitment has led to our 2021-2025 Reconciliation Action Plan being acknowledged by Reconciliation Australia as 'Elevate' – our third RAP to receive this highest level of recognition. We continually push ourselves to be more courageous in our actions particularly in advocating for the Uluru Statement from the Heart.

We look forward to making our contribution towards a new future for Aboriginal and Torres Strait Islander peoples so that they can chart a strong future for themselves, their families and communities. We believe we can achieve much more together than we can apart.

# Contents



©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Confidential

Liability limited by a scheme approved under Professional Standards Legislation.

# Executive Summary

In accordance with the 2023/2024 Internal Audit Plan for the Corporation of the City of Adelaide (CoA), an internal audit focussing on the policies, processes, risks and controls relating to data protection and privacy was performed. The objective, scope and approach for this internal audit project are outlined below.

## Objective

This internal audit project focussed on the assessment of the design of the CoA's process for compliance with relevant privacy legislations and testing the operating effectiveness of key controls such as data management, data storage, privacy breach responses and management, including the way sensitive information is stored, retained and deleted if no longer required. The internal audit included a specific focus on the data protection and privacy practices adopted for the Customer Centre and Community Space areas of the CoA.

## Scope of Services

The scope of this internal audit included consideration over the following areas:

- Review of the design adequacy of the existing privacy policies and processes against the Privacy Act 1988 (Cth), including but not limited to the following areas:
  - Privacy governance structure, including roles, responsibilities and management
  - Privacy policies (Internal/External)
  - Privacy complaints and individual rights management process
  - Privacy incident and data breach management process, including consistency with the Notifiable Data Breach Scheme
- Consideration of the implications of the proposed Privacy Act reforms and any core implications based on the CoA's business model and current state privacy management practices.
- Performed a test of the implementation of privacy and security controls for the Customer Centre and Community Space areas of the CoA. Testing was limited to:
  - Data collection notices, including how consent is obtained
  - Data retention and disposal, complaint management, access and correction request management and data breach management
  - Review the IT application supporting the Community Space and Customer Centre process for the following: Access management, encryption, audit and logging, USB access, and monitoring of personal email access (upload of documents)
  - Privacy Impact Assessment (PIA) or risk assessment processes in place to identify and manage privacy risks arising from new and/or changes in business initiatives/activities.

## Positive Observations

Several positive observations were noted from the CoA's approach to data protection and privacy, which are outlined below:

- Individual rights outlined in both internal and external privacy policies include details on how personal information is to be collected, used, stored and disclosed at the CoA.
- The CoA has implemented sound access management controls based on individuals' roles. An Approving Officer is designated to identify the level of access a user has within the system prior to the Information Management (IM) team providing access. The IM team regularly reviews access to systems and identifies users who are no longer with the organisation or have not accessed the system in the past 90 days.
- Ethical Hacking is performed within the CoA as a proactive measure to identify vulnerabilities and strengthen cybersecurity defences. By simulating cyber-attacks and conducting penetration testing, the CoA can identify potential risks and implement appropriate safeguards to protect its data.
- The CoA demonstrated compliance with PCI DSS (Payment Card Industry Data Security Standard) indicating that the organisation has sufficient security rigor around payment card data. Credit card details are not stored in any of the systems, and controls are in place to ensure employees do not capture or store individual's credit card details as part of the processing of transactions.

## Key Findings and Recommendations

The number of findings identified during the course of this internal audit is shown in the table below with the detailed findings further outlined in this report. Classification of internal audit findings are detailed in Appendix 7. These findings and recommendations were discussed with the CoA Management. Management has accepted the findings and has agreed action plans to address the recommendations.

| Critical | High | Moderate | Low | PIO |
|---|---|---|---|---|
| - | 2 | 3 | 1 | 2 |

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Background

**Australian Privacy Act 1988 (Cth)**

The Australian Privacy Act 1988 (Cth) (the Act) regulates how personal information is collected, used and disclosed by organisations within Australia. The Act sets out the Australian Privacy Principles (APPs), which serve as standards for the collection, use, storage, disclosure, protection and disposal of personal information for Australian APP entities. The CoA has chosen to comply with the Privacy Act and has implemented process, procedures and controls to ensure adherence to the Act.

In 2022, the Federal Government announced a review of the Act, with a view of bringing the Act into the digital age, uplifting protections for personal information, and increasing the transparency and control for individuals over their personal information.

The reforms will remove several existing exemptions and require organisations to adapt their processes and controls to ensure compliance and a proactive stance in data protection. These reforms, and particular areas of potential impact for the CoA, are outlined across key pillars in Appendix 4. Key areas such as redefining personal information, individual rights, notifications and security protocols will be impacted by these changes. By remaining well-informed of these potential changes, the CoA can ensure continued adherence to these evolving regulatory standards.

**Notifiable Data Breach Scheme**

The Notifiable Data Breach Scheme (NDB) is a scheme based on an amendment to the Australian Privacy Act 1988, the Privacy Amendment (Notifiable Data Breaches) Act 2017. Under the NDB scheme, APP entities are obligated to notify individuals and the OAIC when an eligible data breach is likely to impact individuals whose personal information is involved.

As a part of this scheme, organisations must conduct a swift investigation and assessment of a suspected breach, and if confirmed, must notify the affected individuals enabling them to take preventative actions. This mechanism is designed to improve the protection of personal data and to strengthen the trust between the public and organisation that handles personal information.

Currently, the CoA does not have a reporting mechanism within their breach response policies/plans regarding reporting breaches to the OAIC. In addition, the indicative reporting timelines were also not documented (refer Finding 4 for further details).

Interactions with customers are governed by the CoA's Privacy Policy. To support this, further guidelines (Customer Centre - Privacy & Contacting Owners, CHSP Guideline – Confidentiality, Privacy and Information Management) were provided by the business units that were reviewed for this internal audit.

**Overview of the business units reviewed during this internal audit:**

*Customer Centre:*

The Customer Centre team is the first point of contact for customers. Customer Service Officers (CSO) handle phone, email and webform inquiries while Team Leaders provide support and guidance as the primary escalation point for customers. Inquiries are triaged to the respective business unit depending on the inquiry type. In some areas within the organisation, such as the Property and Rates team, a customer may directly contact the business unit.

As a part of their BAU activities, CSO Officers may be required to record customer data which includes, but is not limited to: name, property details, contact details and date of birth. At a high level CSO Officers record basic customer data before triaging the call to the respective business unit where a more detailed inquiry may occur, which may also include the collection of sensitive information. The data is centrally stored within Pathway, the CoA's Customer Relationship Management (CRM) System, and is one of the key systems used by the CoA.

*Community Space:*

Community Space manages the Commonwealth Home Support Programme (CHSP), a national government initiative that provides support services for ageing residents living independently. The services provided range from home maintenance to personal care and nursing. To be eligible for the program, residents are requested to contact MyAgedCare for eligibility screening before redirected to the CoA to further identify what services are required. The CoA has contracted HenderCare to provide services and action job requests raised by the CoA on behalf of the individual.

Due to the nature of the role, Community Space employees are exposed to sensitive customer information such as medical records and income details. Customer data is stored through a third-party service management system called Alchemy SMS. The CoA has an ongoing relationship with Alchemy Technology as the vendor managing the system.

KPMG
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Background (cont.)

The CoA has established a Privacy Policy that aligns, as far as practicable, with the privacy principles outlined in the Privacy Act 1998 (Cth). This policy sets the expectations for individuals as to the CoA's processes for the management of personal information.

**Roles and responsibilities**

While roles and responsibilities are informally defined within the Privacy Policy, through stakeholder interview it was identified that the Risk and Governance team play a role in ensuring both internal and external privacy policies are maintained and accessible. This includes ensuring that employees undergo an annual security training to uphold data security standards and are also overseeing any Personally Identifiable Information (PII) access requests, with four Freedom of Information (FOI) Officers supporting these requests. Enforcement of security and privacy controls is the responsibility of the Information Management (IM) Team which also includes system management and provisioning access for users.

**Policies and Procedures**

To support the privacy governance framework, several guidelines and processes have been developed to assist in privacy management, with ownership of these documents largely managed by the Information Management (IM) team.

Central to these documents are the internal and external privacy policies. Other policies and guidelines used are outlined below:

- IM Work Instruction – User Creation Modification
- Use of Information System Operating Guideline
- BCP & IT Disaster Recovery Plan
- Records Management Operating Guideline
- Unreasonable Complainants Operating Guideline

Although relevant to privacy management, it was noted through stakeholder interviews that an information classification policy or procedure has not been developed due to an internal business decision.

**Individual Rights Management and Complaints**

The Customer Centre Team is the first point of contact for customers. Inquiries or complaints concerning individual's privacy rights are handled by the Customer Centre team before the issue is escalated to the Risk and Governance team for further resolution.

Should a customer decide to request their PII to be accessed or released, an FOI request is raised within the team with one of the four FOI officers assisting the customer, ensuring only the data pertaining to the customer is provided.

**Information Security**

Information Security within the CoA is managed by IM who are responsible for managing and securing the CoA's technological environment. The IM Team is responsible for managing security controls across the systems they manage, including systems that contain sensitive or confidential information. This team also enforces Role Based Access Control (RBAC) with regular reviews conducted to ensure employees have appropriate access levels.

The IM team also monitors document uploads and downloads, preventing unauthorised data transfer and ensuring compliance with the CoA's data security policies. Disposal and retention of Records is overseen by the Records Management Team who work closely with the IM team.

IM serves as the central point for any technology related issues and is the first point of contact when managing cyber incidents or data breaches.

**Third-Party Management**

Procurement of new systems requires IM's input to assess if vendors have sufficient controls with regard to PII. For areas sampled during this review, it was noted that the CoA uses third-party systems as references in their day-to-day activities (for example, Customer Centre uses EzyBill, EzyReg and Community Space (City Lifestyles) uses My Aged Care, My Gov). Additionally, Property & Rates and Community Space (City Lifestyles) have contracted other non-government third parties for key areas of support (which are further outlined in the observation section of this report).

**Training and Awareness**

The CoA employees are required to complete privacy training as part of their onboarding process with a refresher course conducted every two years and enforced by the Risk and Governance team. Within each business unit, specialised training is provided to employees handling sensitive data, such as employees in the Customer Centre and Community Space.

As the first customer interaction point, Customer Centre trains its employees on how to manage customer data, handle customer complaints, verify user identities and how to manage payment card details to remain compliant with PCI DSS. Similarly, the Community Space emphasises obtaining consent and managing PII, considering that the business unit deals with sensitive medical information. Documents and guidelines are available to employees within these units to support adherence to privacy risk management standards.

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Background (cont.)

**Key:** ✓ Positive Observations ⊙ Gaps

As outlined within the scope, two business units were further assessed. The table below provides a summarised overview of the observations that were noted during documentation review and stakeholder interview. Observations were categorised according to KPMG's Privacy Management Framework (as outlined in Appendix 1). The Governance and Operating Model domain is covered separately on page 5 of this report.

| Domain | Community Space | Customer Centre |
|---|---|---|
| **Inventory/Data Planning** | ⊙ Data is stored in Alchemy SMS with the CoA reliant on the vendor to securely store content which is both sensitive and non-sensitive in nature.<br>⊙ Presently there is no inventory/data mapping of the Alchemy SMS as the system is standalone and not integrated into any other system. | ⊙ No Data Mapping/Inventory documentation has been performed. The IM team is currently mapping data stored within each system, however this inventory assessment is currently a work in progress. |
| **Risk, Control and Monitoring** | ⊙ Reliance on Alchemy SMS vendor to manage and mitigate risks.<br>⊙ No Privacy Impact Assessment or initial risk assessment was conducted prior to the procurement of the system or on a periodic basis thereafter. | ✓ The Pathway System is monitored and managed by the IM team and the IM team has oversight over the system. Issues identified within the system are raised to the IM team for remediation.<br>⊙ Initial and ongoing Privacy Impact Assessments have not been conducted for Pathway. |
| **Regulatory Management** | ✓ The CoA is PCI DSS Compliant, with employees informed and advised that credit card details should not be stored within any of the systems or in writing.<br>⊙ Privacy Policy does not identify departments/areas responsible for privacy regulatory management and enforcement. | |
| **Information Lifecycle Management** | ✓ An annual paper-form is provided to customers requesting feedback and update of their personal information. The form is scanned by the Records Management team and is stored in their EDRMS system prior to the form being uploaded to Alchemy SMS.<br>⊙ Customer PII is retained within Alchemy SMS and does not integrate with other CoA systems.<br>⊙ Unused Customer PII is hidden rather than archived, with users still able to access the archived data.<br>⊙ There is reliance on the vendor to adhere to state record disposal schedules. | ✓ Customer PII is collected through the omnichannel contact offerings available in the CoA. Customer data is centrally stored within Pathway.<br>⊙ The current CRM system does not offer single customer view to provide a single source of truth for customer data. Data is siloed with users required to search through the system to identify if there are other interaction points with the customer.<br>⊙ Updates of personal information is ad-hoc within the system. Customer PII is updated when a customer requests it or when a third-party provides more up-to-date data.<br>⊙ Customer data is archived indefinitely within the CoA. |

KPMG
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Background (cont.)

**Key:** ✓ Positive Observations ⊙ Gaps

| Domain | Community Space – City Lifestyles | Customer Centre |
|---|---|---|
| **Policies, Notices and Consent** | ✓ Annual feedback forms provide a disclaimer regarding data collection and references the CoA Privacy Policy.<br>✓ There is a policy outlining the importance of the consent in collecting data as outlined in the Privacy Act 1988 (cth).<br>✓ Processes for obtaining consent and providing notifications are outlined in the CHSP Guideline – Confidentiality, Privacy and Information Management document. | ✓ External Privacy Policy visible and accessible within the CoA's website.<br>⊙ Current call transcripts do not provide recordings or prompts for privacy notifications for customers inquiring via phone calls.<br>⊙ Personal information collection notices are not always provided before or after collecting customer PII. |
| **Incident Management** | ✓ A BCP Plan has been developed for the CHSP program which provides an overview of the potential scenarios, recovery strategies, maximum acceptable outage and key contacts.<br>✓ Cyber incidents related to Alchemy SMS are managed by the vendor with the IM team kept informed. | ✓ BCP/IT DR Plan outlines the process to escalate critical incidents regarding Pathway.<br>✓ Issues with the system generally resolved by IM or escalated to the vendor if IM are unable to resolve them.<br>⊙ A guideline has been developed for unreasonable complaints but the content does not include requirements for privacy related complaints. |
| **Process, Procedures and Technology** | ✓ Alchemy SMS is hosted on the cloud and is regularly patched or updated by the vendor, with the CoA informed about the changes through a newsletter or through a regular meeting cadence.<br>⊙ The CoA is reliant on vendor to manage the system and adhere to current regulatory management and legislation.<br>⊙ Alchemy SMS is not integrated to any CoA systems resulting in data duplication across systems. | ✓ Pathway is integrated to other core systems such as TechnologyOne, resulting in better data quality and accuracy through integrations between systems.<br>⊙ The current CRM system does not offer single customer view to provide a single source of truth for customer data. Data is siloed with users required to search through the system to identify if there are other interaction points with the customer. |
| **Security for Privacy** | ✓ Role Based Access Controls are established within Alchemy SMS. To onboard new users, a form must be submitted to the vendor identifying the access level of the user.<br>✓ Government managed systems, such as MyGov and My Aged Care, are accessed through a secure portal with users able to upload and download the relevant information.<br>⊙ The current Alchemy SMS contract outlines the security controls within the data centre but does not outline what additional controls they have for protection of personal information managed within the system.<br>⊙ Job Requests and care plans containing sensitive information are provided as a pdf attachment in email to HenderCare. | ✓ Role Based Access Controls are established within the organisation and within the Customer Centre space. An Approving Officer within the team identifies the access level of the new user with IM actioning the request.<br>✓ Pathway has audit logs that enable the CoA to generate reports that identify user access to the system.<br>⊙ The single managed inbox for all emails does not enable users to distinguish if content contains sensitive information. Customers are able to send sensitive information with all CSO officers able to access it.<br>⊙ There is no secure platform used to transfer sensitive information to non-government associated third parties and contractors. |

KPMG
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Background (cont.)

**Key:** ✓ Positive Observations ⊙ Gaps

| Domain | Community Space – City Lifestyles | Customer Centre |
|---|---|---|
| **Third-Party Management** | ✓ Contract with HenderCare established by the CoA through its procurement team and addresses key areas of concern in relation to data protection.<br>✓ Monthly account meetings have been established with the vendor to discuss issues or concerns with the system.<br>⊙ Management of Alchemy Technology relies on Community Space team with IM having minimal oversight. | ✓ The CoA utilises government owned systems such as EzyBill and Ezy Reg (parking expiation) to assist in providing their services. Content from these system obtained or uploaded through a secure platform.<br>⊙ Property and Rates currently have a contract with Lanes Communication, a printing agency used for rates notices. Customer details are transmitted through an unsecured email bi-quarterly. |
| **Training and Awareness** | ✓ Privacy training is provided at staff induction with mandatory refresher courses conducted every two years.<br>✓ Additional guidelines and processes in place to ensure Community Space employees obtain consent from customer.<br>⊙ Community Space employees are aware of their obligations regarding consent and collection of customer PII, however there is risk associated with current practice of unsecured transmission of sensitive information to HenderCare. | ✓ Privacy training is provided at staff induction with mandatory refresher courses conducted every two years.<br>✓ CSO officers trained to handle customer inquiries and to record customer data on an as-needed basis only.<br>✓ Credit card details are not recorded physically or within the system and officers are directed to immediately delete any details captured. |

KPMG
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Internal Audit Findings

Internal Audit identified 2 high risk-rated findings, 3 moderate risk-rated findings, 1 low risk-rated finding and 2 performance improvement opportunities (PIO). The details of the findings are provided in the 'Detailed Findings' section of this report. These findings have been individually rated as outlined below. The classifications of risk ratings in this report are based on the CoA's risk ratings (as shown in **Appendix 7**).


| Rating | Ref # | Description |
|---|---|---|
| High | F1 | The CoA's Privacy Governance Framework should be improved and streamlined |
| High | F2 | Inconsistent Information Lifecycle Management |
| Mod | F3 | Insufficient Disclosure of Call Recording Practices and Inconsistent Customer Verification Procedures |
| Mod | F4 | Privacy breaches are not fully addressed in Response Plans |
| Mod | F5 | Security controls managing personal information require strengthening |
| Low | F6 | Privacy Impact Assessments are not conducted on system/applications processing personal information |
| PIO | PIO1 | Frequency of review of privacy framework documentation to be reassessed |
| PIO | PIO2 | Develop an information asset register |

KPMG
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

DRAFT

# Detailed Findings

# Observations and Recommendations

## Finding 1: The CoA's Privacy Governance Framework should be improved and streamlined

**Rating: High**

### Observations

The current internal Privacy Policy lacks a robust privacy governance framework, including assignment of roles and responsibilities and details on reporting. Observations on this finding are noted below:

**A) Privacy roles and responsibilities not documented**

Roles and responsibilities had not been defined and documented within the CoA's internal Privacy Policy. On review of the CoA's Data Management Operating Guideline, key roles and responsibilities associated with data governance and management have not been formally defined, this includes a lack of privacy related responsibilities detailed. Additionally, whilst the document specifies the process and management of data, it does not cover governance of personal information.

Further, issues or escalations around the management of personal information are being managed by the Risk and Governance team. Additionally, the IM team are responsible for assessing any technology related privacy risks. This has the potential to lead to uncertainty or unawareness amongst the CoA staff as to their responsibilities concerning privacy related matters.

**B) Responsibility of enforcement of the Privacy Policy not defined**

Enforcement of the Privacy Policy is not defined, including how privacy management is to be cascaded down to specific departments, individuals or roles within the CoA. Additionally, the Privacy Policy does not detail on how legislative changes are to be monitored and incorporated within the organisation. With changes to the Australian Privacy Act likely to occur in the near future, this gap could lead to potential risks in relation to the management of the regulatory change.

**C) Privacy reporting structure not defined**

The CoA lacks a formal privacy reporting structure from business units to executive leadership and the Council. Management and escalation of privacy issues sits solely with IM or the Risk and Governance team, with no periodic reporting to the Council as defined in the Privacy Policy. This has resulted in limited visibility of overall privacy risk and the potential for siloed approaches in managing privacy related issues.

*(Continued on next page)*

### Recommendation(s)

It is recommended that the CoA:

1. Define the roles and responsibilities of individuals from executive leadership to end-users. Develop a RACI matrix to further define areas that individuals have ownership of and are accountable for.
2. Develop the privacy governance framework structure to include an operating charter that defines the roles, responsibilities and expectations of individuals.
3. Assign a dedicated Privacy Officer to assist with privacy related issues. The Privacy Officer will directly report to a senior leader within the CoA and is expected to champion privacy governance throughout the organisation. This is a recommendation as part of the proposed Privacy Act reforms. Responsibilities should include:
    - Handling privacy related complaints and enquiries
    - Understanding, monitoring and enforcing privacy obligations and regulatory change
    - Assist in conducting privacy impact assessments for new or ongoing initiatives
    - Lead privacy training and awareness initiatives to ensure an understanding of responsibilities regarding privacy governance
4. Develop a structured privacy reporting process (including frequency) to facilitate consistent communication and escalation of privacy matters to the senior leadership and the Council.

### Agreed Management Actions

1. The Privacy Policy will be reviewed and updated to provide defined roles and responsibilities. A RACI model will be developed to further define areas that individuals have ownership of and are accountable for.
2. The CoA will consider developing a privacy governance framework in line with the Privacy Policy.
3. The CoA will assign a dedicated Privacy Officer as part of its response to Recommendation 1 in this finding.
4. A privacy reporting process will be developed in Promapp to facilitate consistent communication and escalation.

**Responsibility:**

1. – 4. Manager, Governance

**Target Date:**

1. 31 December 2024
2. 31 December 2024
3. 31 December 2024
4. 31 March 2025

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

## Finding 1: The CoA's Privacy Governance Framework should be improved and streamlined

**Rating: High**

| Risk(s) | Recommendation(s) | Agreed Management Actions |
|---|---|---|
| *(Continued from the previous page)*<br>• Ambiguity in privacy roles and a lack of clear responsibilities may lead to privacy incidents, improper handling of personal data, and issues in identifying and escalating breaches, posing legal and reputational risks for the CoA.<br>• Absence of documented privacy role definitions undermines accountability, potentially resulting in non-compliance with privacy regulations, especially with forthcoming changes to the Australian Privacy Act.<br>• Inadequate policy enforcement and oversight due to responsibilities resting solely with the CoA without delegation could reduce the effectiveness in identifying and managing privacy related risks.<br>• A siloed approach to privacy issues may hinder the comprehensive management of privacy concerns, resulting in non-compliance with future legislation, and reputational issues. | | |

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

## Finding 2: Inconsistent Information Lifecycle Management

**Rating: High**

### Observations

Management of data is inconsistent across the CoA, with some areas requiring further refinement to reduce privacy risks and inefficiencies. Key areas are noted below:

**A) Limitations in processes to ensure personal information within Pathway is accurate and up-to-date**

The process to update a customer's personal information within the Pathway system is currently ad-hoc, leading to issues in data quality and management. Further, the process heavily relies on customers proactively contacting the CoA to provide updates on their personal details, resulting in outdated customer information being retained in Pathway. Additionally, there is a dependence on third-party services to provide updated customer information, for example, the Property & Rates team uses a third-party system called EzyBill for the management of various electronic billings. Changes in customer details identified through third-party datasets introduces an external risk factor regarding the accuracy and timeliness of updates, as the process relies on the effectiveness of third-party systems.

**B) Retention, archiving and destruction of personal information is inconsistent**

The Privacy Act requires organisations to take reasonable steps to securely dispose of records containing personal information if they are no longer required for the purpose of collection and there are no other legislative requirements mandating organisations to retain the data on a permanent basis. This clause is reflected in the CoA's Privacy Policy but not implemented in practice.

- Employees of the CoA who have access to Pathway are able to view and access customer data that is no longer required for use as part of BAU activities.
- Stakeholder interviews highlighted that users are uncertain as to the process for archiving data within Pathway. Users are aware that records management have some responsibilities regarding this area but assignment of archiving responsibilities between Pathway users and Records Management is not clear and has not been formally defined.
- As the Records Management team and IM have minimal oversight over Alchemy SMS, users are able to access archived data. Archived data in Alchemy SMS relates to customers that are no longer involved in the CHSP program. However, archived data is still accessible and alternative functionality is used to mark these records as hidden.
- CoA personal information records are retained either indefinitely or for a longer period than required. Under the State Records Act 1997, the General Disposal Schedule 40 (GDS40) was developed to provide a guideline on the disposal schedule of council records. However, the CoA retains personal information beyond the retention periods outlined in GDS40. Some examples of this included:
  - 'Visitor books recording visitors to Adelaide Town Hall' are only required to be maintained for ten years by GDS40 however the CoA retains this information indefinitely.
  - 'Records relating to Adelaide City Corporation Awards' are only required to be maintained for two years by GDS40 however the CoA retains this information indefinitely.

*(Continued on next page)*

### Recommendation(s)

It is recommended that the CoA:

1. Establishes policies and processes around data quality. These could include, a formal policy requiring staff to take steps to amend personal information believed to be incorrect based on more up-to-date information, requesting individuals to confirm their personal information when they engage with the CoA, consolidating duplicated records and automated processes to identify personal information that may be incorrect. This should include steps for proactively identifying the need to update out-of-date information or have access to this information restricted until disposal.
2. Ensure sufficient controls are in place to disable read/write/update abilities for customer data that is archived. Further training should be provided to users to ensure that they are aware of the processes to archive data.

### Agreed Management Actions

1. The CoA recognises the importance to have up-to-date data for our customers, therefore, the Privacy Policy will be updated to include guidance on how staff can proactively identify the need for updated customer information. To support this policy update, divisions in the CoA will be communicated the requirement to ensure that, when communicating with customers, the CoA has up-to-date customer information.

   In-line with our actions relating to Recommendation 4, the CoA will first identify what data can be disposed first and impact on duplicate records. Thereafter, the CoA will assess the feasibility of aggregation of records versus a coordinated disposal program.
2. The CoA will review/update the existing Work Instruction (WI-13) regarding appropriate access and permissions to data in pathway.

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

## Finding 2: Inconsistent Information Lifecycle Management

**Rating: High**

### Risk(s)

*(Continued from previous page)*

The inconsistent approach to information lifecycle management may result in the following risks:

- Poor data quality affecting the service provided to customers due to inaccurate records of their personal information.
- Duplication of records within Pathway and across other systems increasing the attack surface of a potential cyber event or data breach.
- Unauthorised alteration of customer information due to staff retaining access to the archived data. In a worst case scenario, this data may be stolen.
- Customer information held by the CoA is not monitored and may be retained for longer than is necessary under applicable regulatory requirements, particularly the GDS40 retention periods. Retaining data for longer than required increases the risk profile associated with unauthorised access, use and disclosure. Furthermore, it can lead to costly data storage and process inefficiencies.

### Recommendation(s)

3. Discuss current security controls with Alchemy Technology to understand their data management process, particularly with how data is disposed.
4. Review and update the data retention schedule for records containing personal information to align with the retention periods stipulated within the GDS40. In the event the CoA determines records containing personal information are required to be retained for longer due to a business need/requirement then the CoA should consider risk accepting the extended retention and/or de-identifying records containing personal information.

### Agreed Management Actions

3. In consultation with Procurement, City Lifestyle team will discuss with Alchemy Technology to understand their data management process in particular with how data is disposed.
4. The Records Management Operating Guideline is currently under its scheduled review. These recommendations will be incorporated into the review.

**Responsibility:**

1. Manager, Governance and Manager, Information Management
2. Manager, Information Management
3. Associate Director, City Culture
4. Manager, Information Management

**Target Date:**

1. 31 December 2024
2. 30 June 2024
3. 31 December 2024
4. 30 September 2024

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

## Finding 3: Insufficient Disclosure of Call Recording Practices and Inconsistent Customer Verification Procedures

**Rating: Moderate**

### Observations

The current process for customer phone enquiries does not provide sufficient notice to customers regarding the recording of the call and data collection. Additionally, inconsistent verification processes were identified, which may pose potential privacy risks. Key areas noted are:

**A) Data collection and recording notice not provided for phone enquiries**

A data collection and recording notice is not disclosed to customers who make inquiries over the phone with the current transcript only describing the process to contact waste services or to remain on the line.

Without clear notifications that calls are records, customers may disclose personal (and potentially sensitive information). Further, a process has not been defined to ensure that notification is provided to a customer, and consent obtained from the customer, prior to the customer providing sensitive information.

The Privacy Act outlines that a collection notification is required, and this notification should include details of the collecting entity, the facts/circumstances of the collection, the purpose of the collection and consequences of not providing personal information. In addition, where a customer provides sensitive information, a process has not been developed to ensure that this notification is communicated, and customer consent is obtained.

**B) Inconsistent verification process**

The verification process of individual's contacting or being contacted by the CoA is inconsistently conducted. The Customer Centre team has a Privacy & Contacting Owners SharePoint page, with the content of this page specifying that PII should not be provided for unauthorised customers for Property and Rates inquiries, however, this does not specify the process that needs to be followed for verifying customers. It was further noted that where customers are verified, this verification process is inconsistently done with some employees requesting additional identifier data while others only require the inquirer's full name. Without an effective, standardised verification process, there is the potential for confidential or sensitive information to be shared with an unauthorised individual, resulting in a privacy breach.

**C) Process to manage privacy complaints not defined**

A defined and documented process is not in place on how privacy related complaints and inquiries are to be handled and escalated within the CoA. This includes escalation to the Privacy Officer and to the Privacy Commissioner, where appropriate.

*(Continued on next page)*

### Recommendation(s)

It is recommended that the CoA:

1. Update the current recording notice to include a statement that the call will be recorded, what the recording will be used for and explicit instructions for the customer to inform the customer centre officer if they would like their call not to be recorded.
2. Provide a disclaimer at the beginning of the call covering the personal information notification information under APP 5. Ensure that training and transcripts are provided to CSOs to obtain explicit consent where sensitive information is collected. Consider whether and how the same disclosure and consent protocols can be applied across other collection channels, e.g. Email.
3. Develop and implement a standardised customer verification protocol across all service agents to uniformly secure personal information. Reinforce this verification process through internal messaging and inclusion in annual training to relevant staff members.
4. Update the Unreasonable Complaints Operating Guideline to include how privacy inquiries and complaints will be handled and escalated within the CoA and externally.

### Agreed Management Actions

1. Agreed.
2. The CoA will implement a disclaimer at the beginning of calls and training and transcripts will be provided to CSOs.

   For other collection channels (e.g. emails), the CoA will investigate how a similar disclaimer can be incorporated and separate action plan to be developed at the conclusion of this investigation.
3. Agreed.
4. Agreed.

**Responsibility:**

1. – 4. Manager, Customer & Marketing

**Target Date:**

1. 31 July 2024
2. 31 July 2024
3. 31 July 2024
4. 31 July 2024

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

## Finding 3: Insufficient Disclosure of Call Recording Practices and Inconsistent Customer Verification Procedures

**Rating: Moderate**

| Risk(s) | Recommendation(s) | Agreed Management Actions |
|---|---|---|
| *(Continued from the previous page)*<br>Although a notification and consent process has been established within the CoA, there are noticeable gaps that needs to be addressed in relation to privacy management, which may result in the following risks:<br>• Failure to take reasonable steps to notify customers of the matters required under APP5, including how their personal data is collected and the purposes of collection.<br>• Sensitive information is collected without valid consent from the individual.<br>• Unauthorised access to sensitive information due to process or control failures.<br>• Failure to manage privacy complaints according to the CoA and/or regulator expectations. | | |

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

## Finding 4: Privacy breaches are not fully addressed in Response Plans

**Rating: Moderate**

### Observations

Privacy incidents that are not directly related to cyber threats are not defined, including investigation and response actions and timelines, including within the CoA's Incident Response Plan and Business Continuity Plan (BCP).

While the existing documentation and BCP/IT DR framework addresses cyber-related privacy breaches, non-cyber related privacy incident scenarios (such as a user mistakenly sending sensitive information to the wrong email address or a list of customer details printed and left out in the open) are not addressed.

Within the Incident Response Plan, identification of a privacy incident is generalised as a data breach. By not distinguishing and addressing specific categories of non-cyber incidents, the CoA risks overlooking and responding to incidents and failing to identify and remediate potential process or control vulnerabilities.

The document also does not address the escalation process to the Office of the Australian Information Commissioner (OAIC), a requirement that has been outlined in the Notifiable Data Breach Scheme. Although a recent incident review noted the need to report to the OAIC, this is not reflected in the incident response plan or in the external facing Privacy Policy, which only calls out the need to inform the OAIC if a Tax File Number data breach has occurred.

Moreover, the document does not set out clear investigation and escalation activities, including associated resolution timeframes, for non-cyber privacy incidents.

### Risk(s)

Due to the insufficient classification of data breaches and the lack of documentation articulating processes for the management of non-cyber privacy breaches, the following risks may occur:

- Personal information breaches (e.g. malicious attacks, unauthorised disclosures, or loss of data) may not be appropriately identified and responded to.
- Failure to update controls where needed in order to prevent similar future breaches occurring in the future.
- Failing to make appropriate and timely notification to the OAIC and affected data subjects.

### Recommendation(s)

It is recommended that the CoA:

1. Update the Incident Response Plan/BCP to include a section detailing what constitutes as a privacy data breach, investigation and communication plans, response timeframes, key contacts and decision makers, and reporting obligations to the Privacy Commissioner. Privacy incidents should be escalated to the Privacy Officer and information security staff.
2. As a part of the annual privacy training, include a scenario regarding a data breach incident (e.g. losing a printed document listing customer data).

### Agreed Management Actions

1. The CoA will develop an Incident Response Plan that addresses a privacy data breach event, including investigation and communication plans, response timeframes, key contacts and decision makers in consultation with IM.
2. Update the Good Governance module to include a scenario regarding a data breach incident.

**Responsibility:**

1. & 2. Manager, Governance

**Target Date:**

1. 30 June 2025
2. 30 September 2024

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

## Finding 5: Security controls managing personal information need to be strengthened

**Rating: Moderate**

### Observations

Although the CoA has implemented preventative and detective security controls throughout the organisation, there are certain areas where controls should be strengthened. Key issue are noted below:

**A) Information classification not defined**

Through stakeholder discussion it was noted that whilst there are guidelines in place, security controls for managing personal information requires strengthening. Upon review of the Records Management Operating Guidelines, it was noted that classification levels for personal information and sensitive personal information had not been defined and documented. These records should have security controls applied commensurate with their risk, such as but not limited to encryption in transit and at rest, access controls, and data minimisation. However, the application of these controls was not consistently applied, and it was unclear how personal information was classified and corresponding controls implemented.

**B) Sensitive personal information provided and received via email**

Through stakeholder discussion it was observed that sensitive personal information is provided to third parties without appropriate security controls applied. Examples cited during the internal audit include:

- The Community Space provides a list of job requests and care plans to HenderCare via email. The data provided contains medical information and is sent as an unsecured pdf attachment, presenting the risk of unauthorised access, modification or disclosure.
- Within the Rates team, customer details are emailed to a third-party printing agency used for rates notices without additional security measures applied, e.g. Encryption or secure file transfer portals. Additionally, the customer centre also receives sensitive information (medical certificate/doctor's notice) via email which is used as evidence to waive parking expiations. This is sent through a single shared inbox enabling all customer centre staff to access or view the document.

### Risk(s)

Inadequate security controls may result in unauthorised access to, and disclosure of, personal information. This may result in the following risks:

- Potential for sensitive information to be misclassified and collected or stored without appropriate technical and organisational security controls.
- Increased risk of privacy incident or breach, particularly with regard to sending the data to the wrong email address or being viewed by an individual without authorisation.

### Recommendation(s)

It is recommended that the CoA:

1. Ensure that information classification protocols include the following:
   - Security classifications addressing personal information
   - Labelling process
   - Business Impact
   - Security controls based on the classification
   - Disposal/Archiving method
2. Develop secure file transfer protocols to share personal information with third parties wherever possible (i.e. where routine sharing occurs).
3. Conduct periodic user access review on shared mailboxes containing sensitive personal information and limit access on a need-to-know basis. This review should leverage existing access reviews, i.e., inactive users, leavers, etc.) but should also include a review of all individuals with access to ensure their access is necessary.

### Agreed Management Actions

1. The CoA will update the existing Data Management Operating Guideline including the review and updating of the data classification categories and controls.
2. IM will investigate Secure File Transfer Mechanisms for the CoA to use with recommendations to be incorporated in the 2025/26 Business Plan and Budget process.
3. IM will develop a procedure to enable regular review of shared mailboxes access and permissions to validate user access by the business owner of the shared mailbox.

**Responsibility:**

1. Manager, Governance and Manager, Information Management
2. Manager, Information Management
3. Manager, Information Management

**Target Date:**

1. 31 December 2025
2. 30 June 2025
3. 30 September 2024

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

## Finding 6: Privacy Impact Assessments are not conducted on system/applications processing personal information

**Rating: Low**

### Observations

The CoA does not currently conduct any privacy risk and impact assessments and privacy risk is not formally considered as part of the risk assessment process.

Specifically, our review identified that new and existing initiatives, including change programs and system implementations, are not assessed as to their impact on personal information management and any new or changed risks presented.

Further to this, the CoA also does not have defined and documented policies, methodologies and supporting templates to conduct Privacy Risk/Impact Assessments (PIAs) on new and existing initiatives that impact personal information. Additionally, no PIAs were evidenced for Community Space and Customer Centre processes or systems/applications, to identify any privacy risks associated with data collection, use, storage, disclosure, etc, along with mitigation strategies to address the risks identified.

### Risk(s)

- Failure to identify and mitigate privacy risks when conducting general risk assessments or designing and implementing change initiatives may result in initiatives being introduced with inadequate consideration of the privacy controls being implemented. This may also result in increased cost of remediation through process or technology debt where programs or projects require redesign to reduce these risks at a later stage.
- Increased likelihood of privacy breaches or incidents due to unidentified vulnerabilities within new projects, processes, or technologies, potentially resulting in unauthorised access to or loss of sensitive data.
- Failing to acknowledge and mitigate privacy risks may lead to non-compliance with data protection laws and regulations, including regulatory censure and fines.
- Overlooking privacy considerations can damage stakeholder trust and customer relations, tarnishing the organisation's reputation.
- Lack of proactive risk management can contribute to inadequate response planning for privacy related incidents, heightening the impact and cost of such events should they occur.

### Recommendation(s)

It is recommended that the CoA:

1. Integrate privacy risk/impact assessments into the broader risk management framework to ensure privacy risks are identified, measured, mitigated and monitored, with sufficient controls implemented to safeguard personal information.
2. Develop and document PIA policy and/or methodology along with supporting templates to ensure that PIAs are considered for new initiatives or projects that may have privacy impacts. The PIA Policy/Methodology should make clear, at a minimum, when a PIA should be conducted, who should conduct it, and how it should be conducted.

### Agreed Management Actions

1. The CoA will incorporate privacy risk / impact assessments into the broader risk management framework, whether it is considered in the operating guideline or the risk register templates.
2. Develop Privacy Impact Assessment methodology with supporting templates to ensure new initiatives or projects consider privacy impacts.

**Responsibility:**

1. & 2. Manager, Governance

**Target Date:**

1. 31 March 2025
2. 31 December 2024

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

**Rating: PIO**

## PIO 1: Frequency of review of privacy framework documentation to be reassessed

| Observations | Recommendation(s) | Agreed Management Actions |
|---|---|---|
| The Privacy Policy is reviewed every three years with the next review scheduled in 2025. While this meets compliance requirements, this may not fully align with better practice. With increasing scrutiny in data privacy and technology, both the internal and external policies are recommended to be reviewed annually to align with better practice. | It is recommended that the CoA annually review the Privacy Policy to ensure compliance with the Privacy Act and any additional regulatory requirements, along with changes to those requirements. | The CoA will conduct an annual review of the Privacy Policy.<br>**Responsibility:**<br>Manager, Governance<br>**Target Date:**<br>31 December 2024 |

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Observations and Recommendations

**Rating: PIO**

## PIO 2: Develop an information asset register (IAR)

| Observations | Recommendation(s) | Agreed Management Actions |
|---|---|---|
| The IM Team is currently developing a document mapping the data stored within each system but only classifies personal information at a high level and does not distinguish the type of personal information stored. Whilst this document will assist the organisation in identifying data integration points, expanding the documentation to include the characteristics of an IAR will help the CoA to identify the data, including personal and sensitive data, held within their environment and associated third parties, along with the risks associated with it and the security controls required to safeguard the data. | It is recommended that the CoA expand the data mapping exercise to build an IAR that includes details of the data held, the owner or custodian of the data, access rights, security classification, and disposal protocols. The IAR should be updated and reviewed by IM regularly to ensure it is accurate and complete, and that sufficient controls are in place to minimise privacy data breach risks. | The CoA will update the existing Data Management Operating Guideline and investigate requirements and expansion of the guideline to incorporate the inclusion of IAR as an appendix.<br><br>Additionally, the CoA will perform a costs and benefits analysis to determine if a project is required to implement security classifications to understand business impacts and value for the CoA.<br><br>**Responsibility:**<br><br>Manager, Information Management and Manager, Governance<br><br>**Target Date:**<br><br>30 June 2026 |

KPMG

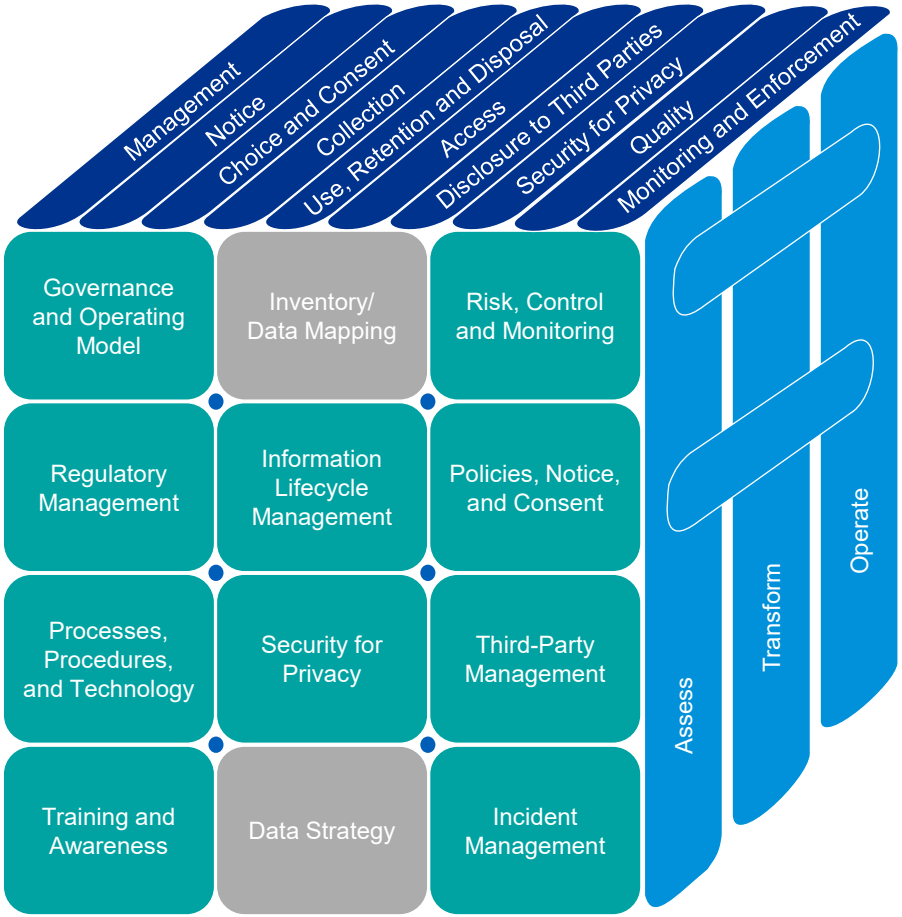
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendices

# Appendix 1 - KPMG's Privacy Management Framework

KPMG has developed its Privacy Management Framework and methodology which includes globally developed best practice privacy principles, combined with our local expertise, to assess your organisation against the Australian Privacy Act 1988 (Cth). The below diagram outlines the areas for consideration when assessing against the KPMG Privacy Management Framework. **Please note that several categories were not in scope (grey), but overlapping observations have been documented and outlined in the Background section of this document.**

| | |
|---|---|
| **Governance and Operating Model** | Establishment of structures, process and governance to oversee privacy management within an organisation |
| **Inventory/Data Planning** | Identification and categorisation of data assets to effectively manage privacy related risks |
| **Risk, Control and Monitoring** | Implementation of measures to assess, mitigate, control and oversee privacy related risks |
| **Regulatory Management** | The management of regulatory obligations and interactions, including regulatory change and regulator interactions |
| **Information Lifecycle Management** | Management of data from the collection to the disposal in accordance with the organisation and regulatory bodies requirements |
| **Policies, Notices and Consent** | Development of privacy guidelines and process to provide open and transparent management of personal information |
| **Incident Management** | Development of an incident management process to respond to privacy breaches or other incidents promptly and effectively |
| **Process, Procedures and Technology** | Establishment of protocols and processes utilising technology to maintain privacy standards and manage personal information |
| **Security for Privacy** | Implementation of security controls to safeguard personal data from unauthorized access or breaches |
| **Third-Party Management** | Management of vendors and contractors to ensure adherence to privacy standards and legislations when handling personal information |
| **Training and Awareness** | Education provided to employees regarding privacy best practices and their roles in protecting data |
| **Data Strategy** | Defines how an organisation collects, manages, analyses, and utilises data to support its overall goals and objectives |




©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendix 2 - Privacy Maturity Levels

Observations during documentation review and stakeholder interviews were noted and assessed against KPMG's Privacy Management Framework and Privacy Maturity Levels. The below diagram provides an overview of the maturity levels that were used to assess against Privacy Management Framework.

**1 Ad-hoc**

- There is evidence that the organisation has recognised that issues exist and need to be addressed.
- Processes are not documented. There are no standardised processes; instead, there are ad-hoc approaches that tend to be applied on a case-by-case basis.
- The organisation is in a state of dynamic change – it is driven in an ad-hoc, uncontrolled, or reactive manner.

**2 Initial**

- Documentation is minimal.
- Processes are repeatable, possibly with consistent results by different people undertaking the same task.
- The organisation lacks rigorous process discipline – there is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
- There is no formal training or communication of standard procedures – responsibility is left to the individual.

**3 Controlled**

- Defined and documented standard procedures are communicated through training and clear roles and responsibilities.
- Risks have been identified, and formal controls operate to ensure effective operation of processes.
- Activities are consistently performed within key functions and business groups, but are not yet coordinated consistently across the organisation.

**4 Monitored**

- Formal processes with review and approval are built in where appropriate, and are communicated consistently across the organisation.
- Activities are consistent and well-coordinated across the organisation.
- KPIs have been defined and are monitored.

**5 Optimised**

- Efficiency and effectiveness of processes is assessed using formal measures and procedures.
- Changes are made to maintain efficiency over time.
- Processes are seamlessly integrated across enterprise boundaries.
- Technology is strategically adopted to reduce cost, effort, and human error in the continuous operationalisation of processes.

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendix 3 - Maturity Rating Against KPMG's Framework

Outlined below is a high level analysis of the CoA's current privacy maturity against KPMG's Privacy Management Framework. It is noted that whilst the majority of the categories overlapped between level 2 and 3, there are several areas where maturity was noted as below that level. **Please be advised that these responses were in consideration of the areas reviewed and have not been validated by KPMG and any operating effectiveness ratings are for illustrative purposes only.**

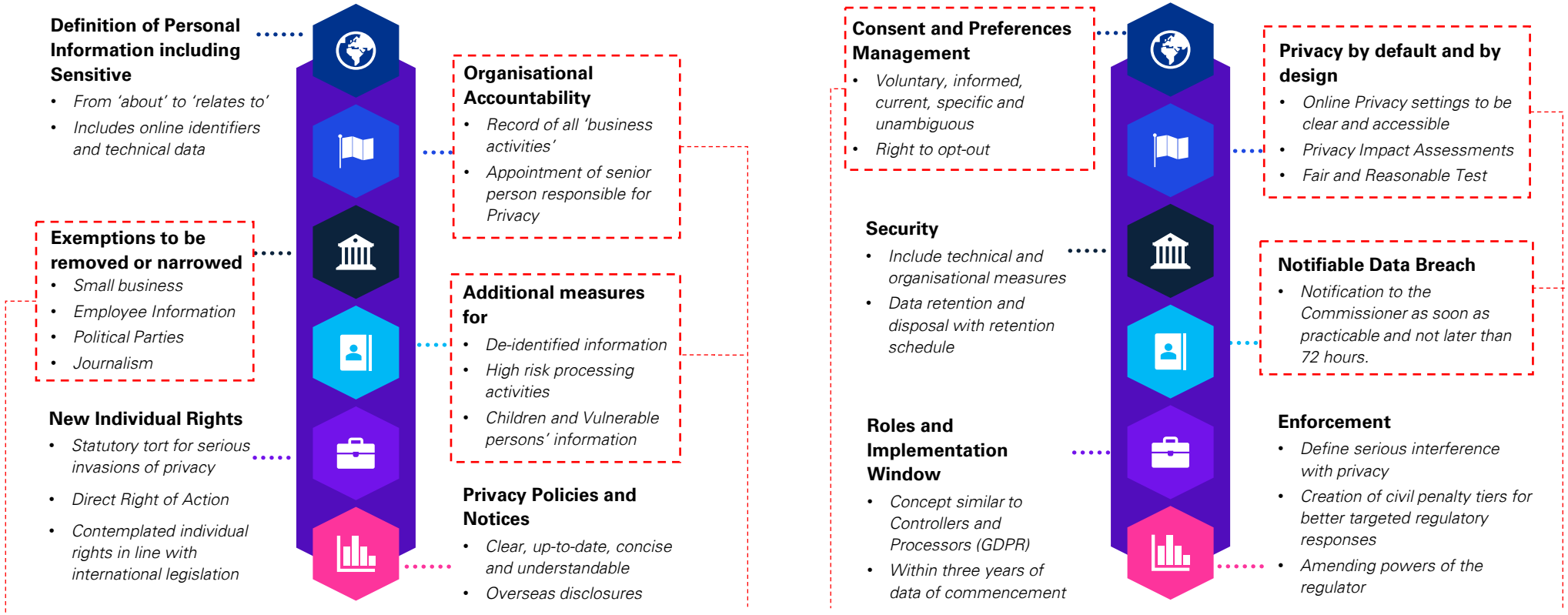
| | Definition | Level 1 | Level 2 | Level 3 | Level 4 | Level 5 | Findings ref |
|---|---|---|---|---|---|---|---|
| **Governance and Operating Model** | Establishment of structures, process and governance to oversee privacy management within an organisation | | ● | | | | F1 |
| **Inventory/Data Planning*** | Identification and categorisation of data assets to effectively manage privacy related risks | ● | | | | | PIO2 |
| **Risk, Control and Monitoring** | Implementation of measures to assess, mitigate, control and oversee privacy related risks | | ● | | | | F6 |
| **Regulatory Management** | The management of regulatory obligations and interactions, including regulatory change and regulator interactions | | | ● | | | F1 |
| **Information Lifecycle Management** | Management of data from the collection to the disposal in accordance with the organisation and regulatory bodies requirements | | ● | | | | F2 |
| **Policies, Notices and Consent** | Development of privacy guidelines and process to provide open and transparent management of personal information | | ● | | | | F3, PIO1 |
| **Incident Management** | Development of an incident management process to respond to privacy breaches or other incidents promptly and effectively | | | ● | | | F4 |
| **Process, Procedures and Technology** | Establishment of protocols and processes utilising technology to maintain privacy standards and manage personal information | | | ● | | | *Refer Background* |
| **Security for Privacy** | Implementation of security controls to safeguard personal data from unauthorized access or breaches | | ● | | | | F5 |
| **Third-Party Management** | Management of vendors and contractors to ensure adherence to privacy standards and legislations when handling personal information | | ● | | | | F5, F6 |
| **Training and Awareness** | Education provided to employees regarding privacy best practices and their roles in protecting data | | | ● | | | *Refer Background* |
| **Data Strategy**** | Defines how an organisation collects, manages, analyses, and utilises data to support its overall goals and objectives | | | | | | |

* Whilst Inventory/Data Planning is out-of-scope, any additional information or observations were noted down.
** Data Strategy is an out-of-scope category and as such, no documentation or questions were asked during stakeholder interviews.

KPMG
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendix 4 - Privacy Reforms

The Privacy Act Review Report 2023 is the culmination of two years extensive consultation which considered whether the Act and its enforcement mechanisms are fit for purpose and outlined proposed changes to the Act. These reforms, coupled with the increase in penalties introduced in 2022, represent a substantial shift in the way data privacy will be regulated in Australia. The following pillars highlight the proposed reforms of the Australian Privacy Act and the potential high-impact areas for the CoA:




With nearly 700 (as at 30 June 2023) FTEs (permanent employees, fixed term temporary employees and common law contract staff) across a broad range of functions and service lines, the CoA will be required to ensure that these individuals are brought within the scope of privacy processes and controls and provided the same protections as customers and members of the community. This is likely to require a refresh of policies, a review of processes and controls and an assessment of systems security protocols as they apply to these individuals.

The Act reforms will require organisations to review and supplement their suite of privacy disclosures, including Policies and collection notices. The CoA will be required to add details of how individuals can request to exercise rights under the Act and how the CoA will respond to requests. The CoA will also be expected to disclose its personal information retention periods as part of its Privacy Policy. In addition, the CoA will be required to determine and record the purposes for which it will collect, use and disclose personal information.

As the CoA services over 26,000 residents and 12,000 businesses, including providing a range of services to vulnerable individuals and collecting sensitive information, there is a significant volume of personal information collected based on consent. As the reforms propose introducing additional requirements for the validity and withdrawal of consent, the CoA will be required to assess all these collection points, determine the fairness and reasonableness of processing activities, and consider whether current practices meet the new standards.

The proposed reforms will introduce a mandate to perform Privacy Impact Assessments for any activities with high privacy risks, requiring the establishment of new processes and control (see F6).

In addition, the revised breach notification timelines, down from 30 to three days, will require the CoA to adapt the incident and breach response plans to ensure that timely investigation and escalation can be performed. The CoA should consider simulation testing to ensure these processes are effective in the event of a breach.

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendix 5- Scope and Approach

**Scope**

The scope of this internal audit considered the CoA's policies, processes, risks and controls relating to Data Protection and Privacy, with a specific focus on the following:

- Review of the design adequacy of the existing privacy policies and processes against the Privacy Act 1988 (cth), including but not limited to the following areas:
  - Privacy governance structure, including roles, responsibilities and management
  - Privacy policies (Internal/External)
  - Privacy complaints and individual rights management process
  - Privacy incident and data breach management process, including consistency with the Notifiable Data Breach Scheme
- Consider the implications of the proposed Privacy Act reforms and any core implications based on the CoA's business model and current state privacy management practices
- Performed a test of the implementation of privacy and security controls for the Customer Centre and Community Space areas of the CoA. Testing was limited to:
  - Data collection notices, including how consent is obtained
  - Data retention and disposal, complaint management, access and correction request management and data breach management
  - Review the IT application supporting the Community Space and Customer Centre process for the following: Access management, encryption, audit and logging, USB access, and monitoring of personal email access (upload of documents)
  - Privacy Impact Assessment (PIA) or risk assessment processes in place to identify and manage privacy risks arising from new and/or changes in business initiatives/activities

**Approach**

This engagement was performed using the following approach:

- Desktop review of the relevant documentation, including policies, procedures, and guidelines relevant to the data privacy methodologies and processes
- Conduct a maximum of four workshops and walkthroughs with nominated stakeholders to understand key data management and privacy policies, processes and controls currently in place, particularly in relation to data protection, storage, classification, information destruction/de-identification and breach management
- Conduct a high level gap analysis of the CoA's current framework/processes against KPMG's Global Privacy Framework
- Reporting, including the identification of any performance improvement opportunities and better practice insights as they relate to the CoA's data privacy framework
- Discussion of findings with Senior Leadership Team
- Drafting and finalisation of an internal audit report outlining internal audit findings, recommendations and any performance improvement opportunities

KPMG
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendix 6 - Stakeholders Consulted

**The table below outlines all personnel who were involved in discussions and contributed to the observations in this report.**

| Stakeholder | Role |
|---|---|
| Jennifer Kalionis | Associate Director, City Culture |
| Steve Zaluski | Associate Director, Regulatory Services |
| David Carroll | Technology, Infrastructure & Platforms Lead |
| Sonjoy Ghosh | Manager, Information Management |
| Martin Smallridge | Manager, Customer & Marketing |
| Alana Martin | Manager, Governance |
| Shaun Coulls | Manager, Commercial & Property |
| Louise Williams | Manager, People |
| Bec Aitken | Team Leader, People Services |
| Janet Crook | Team Leader, Corporate Governance & Legal |
| Daniel Stevens | Team Leader, Marketing & Communications |
| Beth Keough | Team Leader, Community Wellbeing |
| David Burgess | Team Leader, Rates & Receivables |
| Anh Le | Team Leader, Customer Centre |
| Karen Crompton | Team Leader, Customer Centre |
| Jeff Lawes | Senior Assurance and Cybersecurity Analyst |
| Anthony Criscitelli | Office365 Platform Analyst |
| Annette Pianezzola | Risk & Audit Analyst |
| Davin Jaehne | Talent Acquisition Advisor |
| Sadie Goddard-Wrighton | Health and Aging Coordinator |

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendix 7 - Classification of Findings

**The following framework for internal audit ratings is based on the City of Adelaide's risk assessment matrix.**

| Rating | Definition | Examples of business impact | Action(s) required |
|---|---|---|---|
| **Extreme/Critical** | Issue represents a control weakness, which could cause or is causing severe disruption of the process or severe adverse effect on the ability to achieve process objectives. | • Detrimental impact on operations or functions.<br>• Sustained, serious loss in reputation.<br>• Going concern of the business becomes an issue.<br>• Decrease in the public's confidence in the CoA.<br>• Serious decline in service/product delivery, value and/or quality recognised by stakeholders.<br>• Contractual non-compliance or breach of legislation or regulation with litigation or prosecution and/or penalty.<br>• Life threatening. | • Requires immediate notification to the CoA Audit Committee via the Presiding Member.<br>• Requires immediate notification to CoA's Chief Executive Officer.<br>• Requires immediate action planning/remediation actions. |
| **High** | Issue represents a control weakness, which could have or is having major adverse effect on the ability to achieve process objectives. | • Major impact on operations or functions.<br>• Serious diminution in reputation.<br>• Probable decrease in the public's confidence in the CoA.<br>• Major decline in service/product delivery, value and/or quality recognised by stakeholders.<br>• Contractual non-compliance or breach of legislation or regulation with probable litigation or prosecution and/or penalty.<br>• Extensive injuries. | • Requires immediate CoA Director notification.<br>• Requires prompt management action planning/remediation actions. |

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendix 7 - Classification of Findings (cont.)

**The following framework for internal audit ratings is based on the City of Adelaide's risk assessment matrix.**

| Rating | Definition | Examples of business impact | Action(s) required |
|---|---|---|---|
| **Moderate** | Issue represents a control weakness, which could have or is having a moderate adverse effect on the ability to achieve process objectives. | • Moderate impact on operations or functions.<br>• Reputation will be affected in the short-term.<br>• Possible decrease in the public's confidence in the CoA.<br>• Moderate decline in service/product delivery, value and/or quality recognised by stakeholders.<br>• Contractual non-compliance or breach of legislation or regulation with threat of litigation or prosecution and/or penalty.<br>• Medical treatment required. | • Requires CoA Director and/or Associate Director attention.<br>• Requires short-term management action. |
| **Low** | Issue represents a minor control weakness, with minimal but reportable impact on the ability to achieve process objectives. | • Minor impact on internal business only.<br>• Minor potential impact on reputation.<br>• Should not decrease the public's confidence in the Council.<br>• Minimal decline in service/product delivery, value and/or quality recognised by stakeholders.<br>• Contractual non-compliance or breach of legislation or regulation with unlikely litigation or prosecution and/or penalty.<br>• First aid treatment. | • Timeframe for action is subject to competing priorities and cost/benefit (i.e. 90 days). |

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

# Appendix 8 - Disclaimer

## Inherent Limitations

This report has been prepared as outlined in the Scope Section. The services provided in connection with this engagement comprise an advisory engagement, which is not subject to assurance or other standards issued by the Australian Auditing and Assurance Standards Board and, consequently no opinions or conclusions intended to convey assurance have been expressed.

Due to the inherent limitations of any internal control structure, it is possible that fraud, error or non-compliance with laws and regulations may occur and not be detected. Further, the internal control structure, within which the control procedures that have been subject to the procedures we performed operate, has not been reviewed in its entirely and, therefore, no opinion or view is expressed as to its effectiveness of the greater internal control structure. The procedures performed were not designed to detect all weaknesses in control procedures as they are not performed continuously throughout the period and the tests performed on the control procedures are on sample basis. Any projection of the evaluation of control procedures to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

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 City of Adelaide management and personnel consulted as part of the process.

KPMG have indicated within this report the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the report.

KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form.

The findings in this report have been formed on the above basis.

## Third-Party Reliance

This report is solely for the purpose set out in the Executive Summary of this report and for City of Adelaide's information, and is not to be used for any other purpose or distributed to any other party without KPMG's prior written consent.

This internal audit report has been prepared at the request of the City of Adelaide or its delegate in connection with our engagement to perform internal audit services. Other than our responsibility to City of Adelaide, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third-party, including but not limited to City of Adelaide's external auditor, on this internal audit report. Any reliance placed is that party's sole responsibility.

## Electronic Distribution of Report

This KPMG report was produced solely for the use and benefit of City of Adelaide and cannot be relied on or distributed, in whole or in part, in any format by any other party. The report is dated May 2024 and KPMG accepts no liability for and has not undertaken work in respect of any event subsequent to that date which may affect the report.

Any redistribution of this report requires the prior written approval of KPMG and in any event is to be a complete and unaltered version of the report and accompanied only by such other materials as KPMG may agree.

Responsibility for the security of any electronic distribution of this report remains the responsibility of City of Adelaide and KPMG accepts no liability if the report is or has been altered in any way by any person.

KPMG

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

**Justin Jamieson**
**Partner**
T: +61 402 380 169
E: jjamieson@kpmg.com.au

**Heather Martens**
**Director**
T: 08 8236 3273
E: hmartens@kpmg.com.au

**Mischa Steen**
**Associate Director**
T: +61 2 9273 5046
E: msteen2@kpmg.com.au

**KPMG.com.au**

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information
(including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.

Document Classification: KPMG Confidential