Data Protection and Privacy Internal Audit - KPMG

Friday, 14 June 2024
Audit and Risk Committee

Strategic Alignment - Our Corporation

Program Contact:
Kathryn Goldy, Acting Manager Governance

Public

Approving Officer:
Anthony Spartalis, Acting Chief Operating Officer

EXECUTIVE SUMMARY

In accordance with the 2023-24 Internal Audit Plan for the City of Adelaide (CoA), an internal audit was performed to assess the design of the CoA's process for compliance with relevant privacy legislations and to test the operating effectiveness of key controls.

This audit aligns with the Strategic Risk – Cyber Security: Exposure or loss resulting from a cyber-attack or data breach.

The internal audit identified eight findings. Two are risk-rated High, three are risk-rated Moderate and one is risk-rated Low. Two Improvement Opportunities were identified.

The Internal Audit Plan has been developed in consideration of Council's key strategic risks and critical priorities.

Internal audit is an essential component of a good governance framework. It is the mechanism which enables Council to receive assurance that internal controls and risk management approaches are effective, that it is performing its functions legally and effectively, and to advise how it can improve performance.

RECOMMENDATION

THAT THE AUDIT AND RISK COMMITTEE

1. Notes the Data Protection and Privacy Internal Audit report provided as Attachment A to Item 6.2 on the Agenda for the meeting of the Audit and Risk Committee held on 14 June 2024.
2. Endorses the responses of the Administration to the Data Protection and Privacy Internal Audit Report as outlined in Attachment A to Item 6.2 on the Agenda for the meeting of the Audit and Risk Committee held on 14 June 2024.

IMPLICATIONS AND FINANCIALS

City of Adelaide 2024-2028 Strategic Plan	Strategic Alignment – Our Corporation Internal audit is an essential component of a good governance framework. It enables Council to ensure it is performing its function legally, effectively and efficiently.
Policy	Not as a result of this report.
Consultation	Not as a result of this report.
Resource	Not as a result of this report.
Risk / Legal / Legislative	Internal audit is an essential component of a good governance framework. It is the mechanism which enables Council to receive assurance that internal controls and risk management approaches are effective, that it is performing its functions legally, and effectively, and to advise how it can improve performance.
Opportunities	Internal audit focuses largely on compliance, risk management and improvement opportunities. As such audits suggest a range of improvement opportunities related to the area being reviewed, enhancing functions and services and aligning Council processes to best practice standards.
23/24 Budget Allocation	Not as a result of this report.
Proposed 24/25 Budget Allocation	Not as a result of this report.
Life of Project, Service, Initiative or (Expectancy of) Asset	Not as a result of this report.
23/24 Budget Reconsideration (if applicable)	Not as a result of this report.
Ongoing Costs (eg maintenance cost)	Not as a result of this report.
Other Funding Sources	Not as a result of this report.

DISCUSSION

Background

1. The Data Protection and Privacy Internal Audit was performed by KPMG, in accordance with the 2023-24 Internal Audit Plan.

Report

2. This audit aligns with the CoA Strategic Risk – Cyber Security: Exposure or loss resulting from a cyber-attack or data breach.

3. The Data Protection and Privacy Internal Audit 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.

4. The objective of the Data Protection and Privacy Internal Audit included the following:

    4.1. 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:

        4.1.1. Privacy governance structure, including roles, responsibilities and management.

        4.1.2. Privacy policies (internal/external).

        4.1.3. Privacy complaints and individual rights management process.

        4.1.4. Privacy incident and data breach management process, including consistency with the Notifiable Data Breach Scheme.

    4.2. 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.

    4.3. Performed a test of the implementation of privacy and security controls for the Customer Centre and Community Space areas of the CoA. Testing focussed on:

        4.3.1. Data collection notices, including how consent is obtained.

        4.3.2. Data retention and disposal, complaint management, access and correction request management and data breach management.

        4.3.3. Review of 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).

        4.3.4. 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.

5. The findings of the internal audit are indexed into the following risk ratings:

Finding	Risk Rating
The CoA's Privacy Governance Framework should be improved and streamlined	High
Inconsistent Information Lifecycle Management	High
Insufficient Disclosure of Call Recording Practices and Inconsistent Customer Verification Procedures	Moderate
Privacy breaches are not fully addressed in Response Plans	Moderate
Security controls managing personal information require strengthening	Moderate
Privacy Impact Assessments are not conducted on system/applications processing personal information	Low
Frequency of review of privacy framework documentation to be released	Improvement Opportunity
Develop an information asset register	Improvement Opportunity

6. Administration has considered the findings and provided actions and time frames to address these findings.

ATTACHMENTS

Attachment A – Data Protection and Privacy Internal Audit

- END OF REPORT -