Payment Card Industry Compliance Review

Wednesday, 15 May 2024
Audit and Risk Committee

Strategic Alignment – Our Corporation

Program Contact:
Kathryn Goldy, Acting Manager Governance

Public

Approving Officer:
Michael Sedgman, Acting Chief Executive Officer

EXECUTIVE SUMMARY

In accordance with the 2023-24 Internal Audit Plan for the City of Adelaide (CoA) an internal audit on the compliance with the Payment Card Industry Data Security Standard (PCI DSS) was performed.

The internal audit identified fourteen findings of non-compliance during the review.

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 legal, effectively, and to advise how it can improve performance.

RECOMMENDATION

THAT THE AUDIT AND RISK COMMITTEE

1. Notes the internal audit report provided as Attachment A to Item 6.5 on the Agenda for the meeting of the Audit and Risk Committee held on 15 May 2024.
2. Endorses the responses of the Administration to the Payment Card Industry Compliance Review as outlined in Attachment B to Item 6.5 on the Agenda for the meeting of the Audit and Risk Committee held on 15 May 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 Payment Card Industry Compliance Review (PCI Compliance) was performed by Cyber CX, in accordance with the 2023-24 Internal Audit Plan.

Report

2. This audit aligns with City of Adelaide's (CoA) Strategic Risk – Compliance: Non-compliance of Council policies and legislative requirements.
3. The PCI Compliance review provides CoA with an understanding of the level of PCI DSS compliance associated with the payment processing facilities and provides guidance on areas of required remediation following the assessment. This audit is required to be performed annually.
4. The findings of the internal audit are indexed into the following milestones:

Finding	Milestones
Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1
Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	2
Enable only necessary services, protocols, daemons etc as required for the function of the system.	3
Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	2
Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and unnecessary web servers.	3
Maintain an inventory of system components that are in scope for PCI DSS	2
Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	2
Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	2
If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	2
Review the security policy at least annually and update the policy when the environment changes.	6
Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	2
Maintain a list of service providers including a description of the service provided.	2
Maintain a program to monitor service providers PCI DSS compliance status at least annually.	2
Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	2

5. Administration has considered the findings and provided actions and time frames to address these findings as outlined in **Attachment A**. Two of the 14 recommendations have been completed.

ATTACHMENTS

Attachment A – Payment Card Industry Compliance Review

Attachment B – Prioritised Approach

- END OF REPORT -