# Payment Card Industry (PCI) Compliance Update

**Wednesday, 11 December 2024**
Audit and Risk Committee

Strategic Alignment - Our Corporation

**Program Contact:**
Nicole Van Berkel, A/Manager Finance & Procurement

Public

**Approving Officer:**
Anthony Spartalis, Chief Operating Officer

## EXECUTIVE SUMMARY

At the Audit and Risk Committee meeting held 15 May 2024, Administration agreed to provide a six-monthly update to the committee on the progress of the Payment Card Industry Data Security Standard (PCI DSS), Prioritised Approach.

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 in January 2024.

That internal audit identified fourteen findings of non-compliance. Agreed actions addressing eight of these have been completed, with a further six agreed actions still in progress.

## RECOMMENDATION

THAT THE AUDIT AND RISK COMMITTEE

1. Notes the progress of PCI DSS Prioritised Approach as included in Attachment A to Item 4.3 on the Agenda for the Special meeting of the Audit and Risk Committee held on 11 December 2024.

# IMPLICATIONS AND FINANCIALS

| | |
|---|---|
| City of Adelaide 2024-2028 Strategic Plan | Strategic Alignment – Our Corporation<br>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. |
| 24/25 Budget Allocation | Not as a result of this report |
| Proposed 25/26 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 |
| 24/25 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 audit (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 annual PCI Compliance audit provides CoA with advice on the level of PCI DSS compliance of its payment processing facilities, and guidance on areas requiring remediation.

4. The audit's findings and related actions are aligned to 6 milestones defined by the PCI Security Standards Council (Link 1). The table below provides updates on actions completed and those in progress. Since the last update, six actions related to findings were completed, with eight to be actioned by 30 April 2025. Further information on agreed actions addressing the findings is included in **Attachment A**.

| Finding | Milestones | Status |
|---|---|---|
| 1.1.2 Current network diagram that identifies all connections between the cardholder data environment (CDE) and other networks, including any wireless networks | 1 | Completed since May 2024 |
| 1.1.6 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 | In progress due 30/4/25 |
| 2.2.2 Enable only necessary services, protocols, daemons etc as required for the function of the system. | 3 | In progress due 30/4/25 |
| 2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. | 2 | In progress due 30/4/25 |
| 2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and unnecessary web servers. | 3 | In progress due 30/4/25 |
| 2.4 Maintain an inventory of system components that are in-scope for PCI DSS 2 | 2 | In progress due 30/4/25 |
| 9.9.1 Maintain an up-to-date list of devices. The list should include the following:<br>• Make, model of device<br>• Location of device (for example, the address of the site or facility where the device is located)<br>• Device serial number or other method of unique identification | 2 | Completed since May 2024 |
| 11.2.2 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 | Completed since May 2024 |
| 11.3.4 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 | In progress due 30/4/25 |
| 12.1.1 Review the security policy at least annually and update the policy when the environment changes. | 6 | Completed since May 2024 |

| | | |
|---|---|---|
| 12.5.3 Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | 2 | Previously completed |
| 12.8.1 Maintain a list of service providers including a description of the service provided. | 2 | Previously completed |
| 12.8.4 Maintain a program to monitor service providers PCI DSS compliance status at least annually. | 2 | Completed since May 2024 |
| 12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | 2 | Completed since May 2024 |

5. Cyber CX are currently conducting the 2025 annual audit, and will report back on CoA's overall compliance status (reflecting agreed actions taken) by February 2025.
6. Regular updates on CoA PCI DSS compliance are also provided to the CoA's banking provider.

# DATA AND SUPPORTING INFORMATION

**Link 1** - PCI Security Standards Council Milestones

# ATTACHMENTS

**Attachment A** – PCI DSS Prioritised Approach

- END OF REPORT –