Payment Card Industry – Data Security Standards

Follow Up Review

April 2021

Purpose & Background Information

Our original review of Payment Card Industry – Data Security Standards (PCI-DSS) was completed in November 2019 giving a low assurance rating due to the nature of the issues and control weaknesses identified.

It should be noted that the updated opinion is based on the assumption that systems and controls as previously identified during the original audit remain in operation and are being complied with in practice. The purpose of our follow up exercise is not to retest the operation of controls which have already been assessed, but to review how management has responded to the action plans following our initial work.

Audit Opinion

The follow-up identified that progress has been made to implement the agreed action raised, but due to the impact of Covid-19 some implementation dates have been extended. Three of the eight agreed actions have been completed, as follows:

- A report was taken to SLT in December 2019 encouraging corporate buy-in for ensuring corporate compliance with PCI-DSS.
- A cross service Task & Finish Group (T&FG) has been set up and met to discuss a programme or strategy to ensure corporate compliance with PCI-DSS. Workshops have also been held by a specialist PCI consultant to work towards compliance.
- The contract with Denbighshire Leisure is in place and compliance with PCI DSS was included in their obligations.

The remaining five actions have missed the agreed timescales for implementation. This is mainly attributed to the impact of the Covid-19 pandemic on council services and the PCI-DSS consultant's availability. A further follow up review will be needed to establish the progress made with the outstanding actions. Based on the results of our follow up review, we provide a medium assurance rating.

Payment Card Industry – Data Security Standards Follow Up

Assurance Rating

Audit Opinion	Rating
At Final Report	Low ●
At Follow Up	Medium ●

Progress with Implementing Agreed Actions

Action Risk Rating	Actions Fully Implemented	Actions Not Implemented	Actions Not Yet Due
Critical ●	0	0	0
Major ●	2	2	0
Moderate ●	1	3	0

Action Plan Update

Ref	Agreed Action	Issue & Risk	Manager Responsible & Target Date	Follow Up Status and Comments
1.1	Report to the Senior Leadership Team (SLT) to ensure corporate buy-in.	The council does not have a programme or strategy in place to ensure corporate compliance with PCI-DSS. This poses the risk of financial and/or reputation loss and potential withdrawal from payment card acceptance programmes. Major ●	Chief Accountant / Chief Internal Auditor 31/12/2019	Complete Initial report taken to SLT in December 2019 and approved in principle.

1.2	A cross disciplinary Task and Finish Group/Project team will be set up to implement the changes required. The Key services that need to be included in the T&FG include: • Finance • ICT • Information Management • Customer Services • Procurement Service • Service / User Group Representation.	The council does not have a programme or strategy in place to ensure corporate compliance with PCI-DSS. This poses the risk of financial and/or reputation loss and potential withdrawal from payment card acceptance programmes. Major ●	Business and Risk Manager 31/12/2019	Complete A cross disciplinary Task and finish Group has been set up and met. Workshops have been held to address compliance.
1.3	The T&FG will devise a programme which will take account of the issues raised. It is vital that SLT have input into and buy-into the programme as it will impact a number of services. This T&FG will feed into the Information Governance Group to update and monitor progress and escalate any issues.	The council does not have a programme or strategy in place to ensure corporate compliance with PCI-DSS. This poses the risk of financial and/or reputation loss and potential withdrawal from payment card acceptance programmes. Major ●	Task and finish group/ Head of Business Improvement and Modernisation/ Business and Risk Manager 31/10/2020	The T&FG are yet to implement a programme which will take account of the issues raised around the compliance. It has identified the need for an additional module on the income system which will assist compliance on the telephone payment channel. This is on order and waiting on the supplier to implement. Delays

				are due to Covid-19 demands on the supplier's resources. Revised Date 31/09/2021
2.1	The Task and Finish Group to develop and agree training for all relevant staff.	Training provision and record keeping of training is inconsistent and weak in some areas. There is a risk that staff are unaware of requirements to protect cardholders' data resulting in weak security of sensitive personal information. Moderate ●	Task and Finish Group 31/03/2020	All staff that are set up to take card payments have been reminded of their responsibilities around card security A formal training document will be developed once the work with the PCI consultant is concluded, but in the meantime staff will periodically be sent reminders around card security. Revised Date 31/09/2021
3.1	Set up a separate policy or procedures to cover the council's approach to compliance with the PCI-DSS to incorporate procedure to take in the event of a card data breach. This will link to other relevant policies such as the Information Security Policy and Data Protection Policy	Lack of policy or procedure to direct staff towards PCI DSS compliance. Moderate ●	Task and Finish Group 31/03/2020	As previously mentioned, the work with the consultant is ongoing and delayed due to demands on the consultant's time due to Covid-19. Due to the delays with the consultant, a policy or procedure has yet to be developed. Revised Date 31/09/2021
4.1	Cost comparisons with card service providers to be explored. This will need to take	The council's various agreements with card providers may not offer value for money	Task and Finish Group 31/10/2020	Discussions are ongoing in regard to contract extensions which will address the card rate

	into account the full costs, including per transaction costs. A report to be taken to SLT to give assurance that value for money is being achieved. Contracts/arrangements for card payments will be consolidated where possible.	and make it difficult to administer as the card payment environment is more complex that it needs to be. Not only has this resulted in different fees and charges, there is an increased risk of vulnerabilities and non-compliance going undetected. Major ●		issue. Once the new finance system is agreed, it is hoped that the contract can be extended and include the new card rate structure. Revised Date 31/09/2021
5.1	The Task and Finish Group will explore possible measures and update the procurement process (if deemed necessary) to ensure that PCI DSS is always considered when procuring card payment suppliers/services.	PCI-DSS compliance is not always considered as part of procurement or contractual agreements with suppliers that take card payments on behalf of the council. Moderate ●	Task and Finish Group/procurement 31/03/2020	Continual communications between parties whenever systems involving card payments are brought up within the procurement process. Work on this is ongoing and a formal procedure will follow but awareness has been raised and current contracts have been revised to account for PCI (e.g. card payment in public conveniences). Revised Date 31/09/2021
5.2	Include PCI-DSS as a requirements within Denbighshire Leisure's (ADM) contract T&Cs.	PCI-DSS compliance is not always considered as part of procurement or contractual agreements with suppliers that	Legal Services Manager 31/03/2020	Complete The contract with Denbighshire Leisure is in place and compliance with PCI DSS was included in their obligations.

		take card payments on behalf of the council. Moderate ●		

Report Recipients

- Head of Business Improvement and Modernisation
- Head of Legal, HR & Democratic Services
- Chief Accountant/ S151 Officer
- Chief Digital Officer
- Business and Risk Manager
- Business Continuity and ICT Security Officer
- Legal and Procurement Operations Manager
- Team Leader – Communications & Campaign Management
- Corporate Director – Economic and Community Ambition
- Lead Member for Corporate Services and Strategic Direction
- Lead Member for Finance, Performance & Strategic Assets
- Corporate Governance & Audit Committee

Internal Audit Team

Sara Webster, Auditor, 01824 712033, sara.webster@denbighshire.gov.uk

Key Dates

Review commenced	March 2021
Review completed	April 2021
Proposed date for next follow up review	October 2021