PCI DSS

City of York Council

Internal Audit Report 2017/18

Business Unit: Customer and Corporate Services
Responsible Officer: Head of Corporate Finance & Commercial Procurement Manager
Service Manager: Systems Accountant
Date Issued: 18 January 2018
Status: Final
Reference: 10260/024

	P1	P2	P3
Actions	**0**	**0**	**2**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is an international standard mandated by the five major card issuing brands - Visa International, Mastercard, American Express, Discover, and JCB. They have collectively adopted PCI DSS as the requirement for all organisations which process, store or transmit payment cardholder data.

Payments accepted using any debit, credit, or pre-paid card from these issuers are subject to the PCI DSS. While all merchants, regardless of their size or the value or volume of transactions, need to be PCI DSS compliant, the specific compliance regime applicable to individual merchants does depend on these factors. The merchant remains responsible for looking after its customers' card data, regardless of who processes the data on the merchant's behalf.

Penalties for non-compliance can be severe. The payment brands may, at their discretion, issue monthly fines to the acquiring bank for PCI DSS compliance violations. Banks usually pass these fines on to merchants, and may also terminate a merchant's ability to process card payments, or may increase their transaction fees. In the event of a data breach, merchants may also be liable for all of the costs of the forensic investigation, which can run into thousands of pounds.

In addition, breaches involving personal data fall within the scope of the Data Protection Act 1998, and the Information Commissioner's Officer may impose penalties over and above any action taken by the card issuers.

The 2016/17 audit examined the arrangements within the council for ensuring that compliance with the requirements is achieved and maintained. It did not include a technical review of compliance with the standard of the council's operational procedures, IT systems or networks, as many of these aspects had been covered by the Information Security Gap Analysis provided by external consultants (Random Storm) in August 2014.

The audit highlighted a number of issues which were discussed with responsible officers and an action plan was subsequently agreed.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system ensured that the action plan agreed has been implemented, namely:

- Compliance roles have been formally documented and responsibilities are clear.
- The cardholder data environment has been defined, including mapping processes and transactions subject to the PCI DSS
- The council has developed a policy to manage compliance with the PCI DSS, including operational procedures and guidance/training notes for staff to ensure compliance of internal payment processing activities have been developed.

- Responsibility for monitoring third party processors has been assigned.
- The council has a co-ordinated process to ensure that all relevant annual self-assessment questionnaires are completed accurately and submitted on time.

The audit did not include review of the technical compliance of the authority's IT systems and networks with the PCI DSS.

Key Findings

From the work undertaken, it is evident that significant steps have been taken to ensure the Council's compliance with the PCI DSS.

A formal PCI DSS Security Policy has been developed and has been distributed to all managers and employees responsible for taking card payments on behalf of the Council. The Policy was reviewed against available best practice advice, and appears to be complete, accurate and useful. Paragraphs 6 to 18 outline procedures for staff that are responsible for taking card payments. Managers are required to ensure that they (and their staff) are comfortable with the requirements of the Policy with a signature of acknowledgement required. Further training will be provided to staff by March 2018. This will need to followed-up (see Action 1 at the end of this report). However, due to the difficulties in organising the training for the current year, the mitigating action taken is considered sufficient for the short-term.

Roles and responsibilities for ensuring that the Council is PCI DSS compliant have been assigned, with ultimate responsibility falling to the Systems Accountant who is assisted by the Financial Transactions Manager and the ICT Infrastructure Manager. These roles are outlined in Paragraph 5 of the PCI DSS Policy.

The Council has created a PCI DSS Asset Register to document and monitor systems and processes subject to the PCI DSS. This includes a list of all merchant devices utilised by the Council, each with an assigned responsible officer and the volume and value of transactions processed by the device. Some volume and value totals for individual merchant machines are not currently available due to the data from Global Payments (HSBC's card provider, utilised by the Council) being unavailable. Once the reporting tool can be accessed by the Financial Transactions Manager, this will be followed up as outlined in Action 2.

The Asset Register is utilised by the Financial Transactions Manager to monitor due dates for PCI DSS compliance certificates' renewal. This ensures that third-party payment processors submit their compliance with the PCI DSS to the Council in a timely fashion and assists in monitoring the various dates the certificates are valid until. As part of the work undertaken on this audit, certificates were examined for all processors acting on behalf of the Council. No exceptions were identified and proof of monitoring was evident on the Asset Register. The Council utilises Security Metrics, a compliance tool, to accurately fill out the required self assessment questionnaire (SAQ), significantly reducing the complexity of the process. The results of the most recent assessment were examined and show the Council to be PCI DSS compliant.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Training

Issue/Control Weakness	Risk
PCI DSS training has not yet been provided to all staff members responsible for taking card payments on behalf of the Council.	The council does not have a strategy or policy to help manage compliance with the PCI DSS. Operational procedures and guidance notes for staff to ensure compliance of internal payment processing activities have not been developed.

Findings

PCI DSS training has not yet been provided to all staff members responsible for taking card payments on behalf of the Council. This training has been delayed due to procurement issues related to selecting the correct training provider. The Financial Transactions Manager and ICT Infrastructure Manager have now selected a training provider, and training will have been provided by March 2018.

Agreed Action 1.1

Training will be provided to staff responsible for taking card payments.

Priority	3
Responsible Officer	Financial Transactions Manager
Timescale	30 March 2018

2 Volume and Value Totals

Issue/Control Weakness	Risk
Some volume and value totals for individual merchant machines are not currently available.	The council has not documented and assessed for compliance all processes which may be subject to PCI DSS requirements.

Findings

Some volume and value totals for individual merchant machines are not currently available due to the data from Global Payments being unavailable. When the reporting tool can be accessed by the Financial Transactions Manager, this Asset Register must be examined to ensure all volume and value totals have been accurately recorded.

Agreed Action 2.1

The Financial Transactions Manager will ensure that electronic volume and value totals are made available by Global Payments and will update the register accordingly.

Priority	3
Responsible Officer	Financial Transactions Manager
Timescale	30 March 2018

Audit Opinions and Priorities for Actions

Audit Opinions
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.