Veritau
Assurance Services for the Public Sector

PCI DSS

Selby District Council

Internal Audit Report 2017/18

Business Unit: Corporate
Responsible Officer: Director of Corporate Services & Commissioning
Head of Service: Head of Business Development & Improvement
Service Manager: Data & Systems Team Leader
Date Issued: 12 July 2018
Status: Final
Reference: 76470/001

	P1	P2	P3
Actions	**1**	**0**	**0**
Overall Audit Opinion	Limited Assurance		

Summary and Overall Conclusions

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is an international standard that was introduced by the five major card issuing brands (Visa International, Mastercard, American Express, Discover and JCB) to ensure that all organisations that process, transmit or store card payments do so securely.

Payments accepted using any debit, credit or pre-paid card from these issuers are subject to the standard. While all merchants – irrespective of the size, 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 card issuing brands may, at their discretion, impose monthly fines on the acquiring bank for PCI DSS compliance violations. Banks usually then pass these fines on to merchants. They may also terminate a merchant's ability to process card payments or increase their transaction fees. In the event of a data breach, merchants could also be liable for all of the costs of the forensic investigation which can run into thousands of pounds. In addition, breaches that involve personal data fall within the scope of the Data Protection Act 1998 and the Information Commissioner's Office may enforce penalties over and above any action taken by the card issuers.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that effective controls have been put in place to manage compliance with the PCI DSS. It will cover the following key elements of compliance, to establish whether the Council has:

- documented all systems and processes subject to the PCI DSS
- compliance assurance processes in place from third-party payment processors acting on its behalf
- up to date guidance in place for all Council staff who process card payments
- submitted annual self-assessment questionnaires and attestations of compliance with PCI DSS

The audit did not include a detailed technical review of operational procedures, IT systems or networks. It did, however, include a high-level review of the existing cardholder data environment and its compliance with the standard. It also included follow up the actions that were agreed during 2016-17 to ensure that the issues and control weaknesses had been satisfactorily addressed.

Key Findings

The Council engaged a specialist information security consultant in May 2016 to advise on its compliance with the PCI DSS. The consultant's report concluded that the Council is not compliant with the standard and that its entire network and all staff are within scope. The configuration of the network has remained unchanged since the publication of the report. There is no secure segmentation of the Council's cardholder data environment and, therefore, the PCI DSS security requirements extend to all network components. The nature of the network (including its being hosted by North Yorkshire County Council) means that addressing compliance gaps is likely to be impractical but there are some scope reduction options available. No corporate decision has been taken as to which (if any) of the scope reduction options recommended by the consultant will be pursued. Part of the reason for this is that an appropriately senior officer has not been identified as responsible for ensuring the security of card payment processing.

A draft PCI DSS compliance policy has been developed. The content of the policy was found to be generally adequate but there are a number of improvements that could be made and the document will require a thorough review to ensure that it aligns fully with the Council's card payment processing activities.

The volume of the Council's e-commerce transactions means that is at Merchant Level 4, the compliance validation regime of which includes quarterly network penetration scans and completion of an annual self-assessment questionnaire. The Council has not yet completed a self-assessment questionnaire and has not made arrangements for the performance of quarterly network penetration scans.

Overall Conclusions

The arrangements for managing risk were poor with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided Limited Assurance.

1 Scope of the cardholder data environment

Issue/Control Weakness	Risk
The scope of the Council's PCI DSS compliance is all systems as there is no secure segmentation of payment processing.	A data security breach in one area of the network could lead to a breach in another.

Findings

The Council has four channels for card payment processing:

1. Telephone payments received at both the Customer Contact Centre and the Civic Centre
2. Payments received through the website
3. Payments received through the Interactive Voice Response (IVR) system
4. Payments received through payment kiosk (SCAN COIN) in the Customer Contact Centre

During the 2016/17 financial year, payment card transactions were as follows:

Payment channel	Number of transactions	Value of transactions
Telephone	16,335	£2,325,838.27
E-commerce (web)	5,066	£804,268.24
IVR	13,256	£2,043,902.66
Kiosk	14,679	£1,642,099.43
Total	**49,336**	**£6,816,108.60**

The specialist information security consultant engaged in May 2016 reported that the Council's network configuration was such that it was not compliant with the PCI DSS and that the scope of compliance extended to its entire network due to the lack of secure segmentation. No changes have been made to the cardholder data environment since publication of the report.

Payments are processed by the Council through a number of desktops based at both the Customer Contact Centre and at the Civic Centre which puts the network on which these reside in scope as there is no segmentation from the rest of the network. The telephony system uses Voice Over Internet Protocol which also brings this network into scope. The PARIS cash receipting system is part of the cardholder data environment as card data is sent to the PARIS APACS server which is on the Council's network. There are uncertainties around whether or not the SCAN COIN kiosk uses the Ethernet network to make payments. If it does use the network then the Council could be considered a service provider (processing, sorting or handling card information on behalf of the kiosk supplier).

While it would likely be impractical to attempt to bring all networks and staff into compliance with the standard, there are mechanisms for segmentation and changes in business practices which would reduce the scope of compliance.

Consideration should also be given to the wider network environment within which the Council's network resides. As part of the Better Together partnership, the Council has shared ICT and telephony infrastructure with North Yorkshire County Council (NYCC). Although the data flows were not verified during the audit, it is highly likely that cardholder data processed by each of the Council's four payment channels will come into contact with, and possibly be stored on, NYCC's network.

The council does not currently have assurances from NYCC that its own network configuration is such that it adequately safeguards the cardholder data that it effectively processes on behalf of Selby District Council as a third party service provider. What this means is that, while the Council can takes steps to ensure that its internal processes are compliant with the PCI DSS, its cardholder data is still at risk were the NYCC network to be breached.

Agreed Action 1.1

Data & Systems will seek assurances from NYCC as to the compliance of their cardholder data processing and liaise with the new income management system software supplier to better understand the future of PARIS and possible opportunities for scope reduction. An options appraisal will then be presented to Leadership Team which will set out the risk and cost implications of pursuing changes to the existing cardholder data environment. As for the compliance validation requirements, responsibilities will be established and assurances will either be obtained from NYCC that compliance requirements are being fulfilled or arrangements will be put in place to ensure that Selby District Council fulfils its requirements.

The content of policy and procedures for PCI DSS will be influenced by the option chosen by Leadership Team. Once a corporate decision has been taken the policy and procedures will be developed accordingly.

Priority	1
Responsible Officer	Head of Business Development & Improvement
Timescale	September 2018

2 Policy and procedures for PCI DSS compliance

Issue/Control Weakness	Risk
The Council has not agreed a strategy or policy to help manage compliance with the PCI DSS. Operational procedure notes for staff to ensure compliance of internal payment processing activities have not been developed.	Non-compliance with the PCI DSS, leading to the potential imposition of fines, increased transaction charges, or suspension of ability to process card payments.

Findings

At the time of the audit a PCI DSS compliance policy was in development but had not been approved and circulated to staff. The content of the draft policy was reviewed against available good practice and against good practice for policy writing more generally. While the content of the policy was found to be adequate overall, there are a number of notable omissions. These include:

- A policy owner
- Version control (including revision history)
- Arrangements for fulfilling compliance validation requirements
- Arrangements for data security incident response
- Third party compliance requirements and monitoring

In general, the document requires a thorough review to ensure that the policy, including the appended declaration, aligns with the Council’s existing card payment processing activities and with its structure, roles and responsibilities.

Sections 6-10 of the policy and the appended Departmental PCI DSS Declaration clearly define expectations in respect of card payment processing, data handling, retention and physical security of card processing equipment. The policy and declaration are together prescriptive and effectively serve as procedures. A full understanding of the policy (and declaration to that effect) should ensure that officers are sufficiently aware of their responsibilities when processing card payments.

Agreed Action

Please refer to Agreed Action 1.1.

3 Compliance validation requirements

Issue/Control Weakness	Risk
The validation requirements for a typical Merchant Level 4 compliance regime are not being fulfilled.	Non-compliance with the PCI DSS, leading to the potential imposition of fines, increased transaction charges, or suspension of ability to process card payments.

Findings

The number of ecommerce transactions processed annually means that the Council is currently at Merchant Level 4. Although the validation requirements are ultimately set by the acquiring bank, the typical compliance regime for this Merchant Level involves completion of the relevant annual Self-Assessment Questionnaire, performance of quarterly network penetration scans by an Approved Scanning Vendor and submission of the relevant Attestation of Compliance form.

The Council part completed a Self-Assessment Questionnaire prior to the information security consultant coming on site in May 2016 but their advice was not to complete the submission (i.e. to also include the Attestation of Compliance form) until changes had been made to its networks. The consultant’s report included several options to reduce the scope of compliance through segmentation and through changes to business processes but, while the feasibility of some options have been pursued, a corporate decision has not yet been taken as to the desired configuration.

Arrangements have not been made for the performance of quarterly network scans by an Approved Scanning Vendor.

Agreed Action

Please refer to Agreed Action 1.1.

Annex 1

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.