PCI DSS (Payment Card Industry Data Security Standard)

City of York Council

Internal Audit Memo

Service Area:	Cross Cutting
Responsible Officer:	Director, Customer & Corporate Services
Service Managers:	Corporate Finance & Commercial Procurement Manager Head of ICT
Date Issued:	15th March 2017
Status:	Final
Reference:	10245/008

1.0 Introduction and scope

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 standard. 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.

This review 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 have been covered at least in part by the Information Security Gap Analysis provided by external consultants (Random Storm) in August 2014.

The corporate finance team, the Head of ICT and the ICT Infrastructure Manager have provided information for this review.

A draft report was originally issued in April 2016. The findings from this have been discussed with officers along with some initial recommendations. An action plan has subsequently been agreed.

2.0 Initial findings

2.1 Senior management responsibility for PCI DSS compliance

Payment card processing is carried out by various service areas within the council. Currently there is no senior manager who has been made formally responsible for overall PCI DSS compliance and who would co-ordinate the input from managers in relevant service areas, such as Finance, ICT or Customer Services. The main compliance steps to date have been taken by the Financial Transactions Manager (Corporate Accountancy) and the ICT Infrastructure Manager, as they recognise the risks to the council of non-compliance, but their efforts do not form part of a systematic council-wide approach.

As well as addressing the compliance of current card payment processing, the council needs to implement a process by which changes to the requirements of the standard, or in systems and processes subject to the standard, are recognised and acted upon promptly. Compliance with the standard should also form part of procurement and transformation processes, as apparent savings and efficiencies in new payment processing methods can easily be cancelled out by more onerous compliance regimes which may result from them.

There is also often a misconception within organisations that PCI DSS is primarily an ICT issue, and while ICT security does play a key role in compliance, there are many other equally significant aspects which fall outside the remit of an ICT department.

- Compliance roles have not been formally documented, and responsibilities are unclear. As a result, ongoing compliance with the standard is not thoroughly assessed by the council, and changes to the requirements of the standard, or in systems and processes subject to the standard, may not be recognised and acted upon.

2.2 Defining the cardholder data environment - mapping processes and transactions subject to the PCI DSS

The council does not have any up to date document which records the various methods in which it processes payment card data, and does not monitor the total number of card transactions per year, which also has a bearing on compliance requirements for merchants, particularly if the number of transactions for each merchant account is aggregated. The standard also requires that an inventory be maintained of devices which are in its scope. Mapping processes, transactions and data flows would allow the council to create this inventory.

The gap analysis carried out by Random Storm in 2014 provided useful information on data flows for different methods of payments processing, and guidance on what could be in scope for PCI DSS. It should however be noted that a new version of the standard (v3.1) has been issued since the gap analysis was conducted. Since then the council has also made changes, and is planning further changes, to systems within the cardholder data environment, such as the introduction of payment kiosks at Park and Ride sites and changes to telephone call handling systems to prevent cardholder data from being recorded.

It is also important to consider whether legacy cardholder data from earlier processing methods may still reside on the council network. Whilst the ICT Infrastructure Manager is confident that redundant databases have been removed, there is always a possibility that spreadsheets or other documents created by individuals or teams within service areas may exist, which would also be within the scope of the standard. At least one organisation has been heavily penalised for failing to ensure that legacy data are protected.

- Without documenting the various systems, processes, staff roles, and pieces of equipment which are involved in receiving card payments, it is difficult for the council to determine whether compliance self-assessment questionnaires are being completed accurately, and with an awareness of the wider requirements of the standard, such as regular network security scans by an approved scanning vendor.

2.3 Policies, procedures and training for PCI DSS compliance

There is no strategic document in which the council sets out how it will manage compliance. To achieve and maintain PCI DSS compliance, an organisation must "Establish, maintain, and disseminate a security policy". This would relate its operations to the requirements of the standard.

The standard also requires that organisations "Educate personnel upon hire and at least annually", if they process card payments, and also "Provide training for personnel to be aware of attempted tampering or replacement of devices". The Financial Transactions Manager (Corporate Accountancy) offers informal guidance to users of PDQ ('Process Data Quickly') terminals, but service areas have not developed operational training or procedure notes for their staff involved in payment card processing, to ensure that processing does not pose any risk to cardholder data.

- The council has no strategy or policy to manage compliance with the PCI DSS. Operational procedures and guidance/training notes for staff to ensure compliance of internal payment processing activities have not yet been developed.

2.4 Compliance assurances from third parties

The council relies on a number of third parties for payment processing, but their ongoing compliance is not monitored. The standard states "Merchants and service providers must manage and monitor the PCI DSS compliance of all associated third party service providers with access to cardholder data".

For example, when a consumer wishes to make a payment online and visits the council website, they are redirected to a different web site provided by Civica. The council must obtain annual assurance that the Civica element is compliant, and also put in place the appropriate compliance actions for its website. In this example, an attacker could compromise either of the websites. They could amend the links which cause the user to be redirected from the council site, and have these point to the attacker's fake payment page, rather than to the genuine Civica pages. The attack could also be carried out directly on the Civica servers.

As a further example, the council has car park ticket machines which accept card payments, but again it is unclear who is responsible for their compliance, such as carrying out checks required by the standard that they have not been tampered with, perhaps by having a "skimmer", or card reader, attached by criminals.

- All such dependencies will need to be explored fully by the council as part of the compliance process. Responsibility for monitoring them needs to be assigned.

2.5 Completion of annual self-assessment questionnaires

Self-assessment questionnaires (SAQs) are an attestation by the council that all of its payment card processing activities are compliant, and must be completed annually. The number and types of questionnaires are usually determined by the nature of the card processing undertaken, the number of transactions and/or the number of merchant accounts held by the merchant.

The council does not have a co-ordinated process to ensure that all relevant annual self-assessment questionnaires are completed accurately and submitted on time. They are currently the responsibility of individual finance officers - the Financial Transactions Manager (Corporate Accountancy) usually completes twelve questionnaires covering PDQ payment channels, as there are twelve separate merchant accounts. The Accountant (CANS & CES Finance) usually completes a questionnaire for the PayByPhone payment channel relating to car parking.

We could not establish whether the council submits all relevant questionnaires. There may also be scope to rationalise the number of merchant accounts, and therefore the number of questionnaires which the council needs to submit.

- The completion of some annual self-assessment questionnaires may be outstanding. Questionnaires may not be completed with a full knowledge of the requirements of the standard.

3.0 Conclusion

3.1 The council has taken some steps towards compliance, but these are fragmented and are due to the diligence of individual officers, rather than any co-ordinated corporate approach. The council has little documented assurance that its processes and systems are sufficiently robust to protect cardholder data. Beyond pockets of knowledge in ICT and Finance, awareness of the PCI DSS is limited, as little work has been undertaken by the whole of the council to assess its internal operations against the requirements of the standard.

3.2 While these third parties must indeed be compliant, the standard states “Merchants and service providers must manage and monitor the PCI DSS compliance of all associated third party service providers with access to cardholder data". Therefore it is the council’s responsibility to ensure that its implementation of ICT systems is compliant, that the equipment, systems and services provided by third parties are compliant, and that all of its associated non-ICT processes, such as handling of hard copies of cardholder data, are compliant.

3.3 Cardholder data may therefore be exposed to the risk of loss or theft, which in turn exposes the council to the risk of the sanctions and penalties discussed above.

4.0 Initial Recommendations

4.1 The council needs formally to assign overall responsibility for achieving and maintaining compliance to an officer with sufficient seniority to co-ordinate the input and efforts of managers from the various service areas which are involved in card payment processing.

4.2 All processes by which the council receives income from payment cards, and the total number of transactions per year, need to be determined. These include where payments are processed by third parties. The council needs to establish whether the number of transactions from the various merchant accounts should be aggregated.

4.3 The council should use this information to select the relevant SAQs, which set out the requirements of the standard depending on how cardholder data are processed. Further specific help and advice should also be available to the council for each merchant account from its provider.

4.4 Based on this, and the further information set out on each of these areas in the standard itself, the council should develop and disseminate suitable procedure notes for staff, to ensure that working practices are compliant.

4.5 An overall strategic approach also needs to be developed, to ensure that any future changes in the standard, or in the ways in which the council processes payment cards, are recognised and promptly assessed for their impact on compliance. Choosing payment processing methods which outsource most of the compliance issues could massively reduce the burden on the council, and this factor should form part of any process of choosing future payment processing systems.

4.6 These actions need to be drawn together in a policy which sets out how the council will manage compliance activities.

4.7 Once compliance is felt to have been achieved in each area, the appropriate SAQs need to be completed and submitted annually, supported by any other compliance activities which may be required, such as network scans/penetration testing. Often the submission is made online, using electronic forms supplied by the merchant account's PCI security contractor.

4.8 Veritau would be happy to provide further advice and support in these areas, so that the council can develop procedures to assess its compliance status and take remedial action where necessary.

5.0 Agreed Actions

5.1 Senior management responsibility for PCI DSS compliance

The Systems Accountant (Graham Frodsham) is the corporate responsible officer, although this is not currently documented anywhere. He is being supported by the Financial Transactions Manager (Corporate Accountancy) (Allan Barton) and the ICT Infrastructure Manager (Paul Robinson). This will be formally documented in due course.

5.2 Defining the cardholder data environment - mapping processes and transactions subject to the PCI DSS

In the embedded spreadsheet the council has identified and listed all areas which process cards, and has further broken this down by merchant numbers. The number of transactions for each merchant number and a responsible officer have been determined. This involved consulting income records and the council will continue to monitor this annually.

The council intends to develop a full inventory of devices in scope for PCI DSS.

PCI Compliance - Asset Schedule.xlsx

5.3 Policies, procedures and training for PCI DSS compliance

The council has not yet developed these, although it has approached neighbouring authorities about their training and policies.

The council also obtained sample policy documents from Veritau and intend to develop their own versions tailored to the council. As an interim measure they will refer to the need for PCI DSS compliance in the council's Information Security Policy.

5.4 Compliance assurances from third parties

Some certificates have now been obtained and their validity dates are recorded in the spreadsheet embedded above at 5.2.

Once the compliance policy documents are completed and the council has full clarification of compliance responsibilities between third parties and the council (in a policy, for example), the council will continue to monitor third party compliance as appropriate.

5.5 Completion of annual SAQs

The Financial Transactions Manager (Corporate Accountancy) has submitted an SAQ online via Security Metrics (the bank's compliance contractor), which covers the chip-and-PIN payment channel. (He used to make multiple submissions, so this has been rationalised as suggested.) He has informed Security Metrics of other payment channels.

As the SAQ Instructions and Guidelines state "Merchants with more than one channel should consult with their acquirer about how to validate compliance", the council will seek further clarification and document the outcome in their policies.

6.0 Conclusion

6.1 Since our original report, the council has taken several positive steps towards creating a process to achieve and maintain compliance. Further actions have been agreed and initial work will be undertaken on these by 30/04/2017.

6.2 Progress against these actions will be followed-up by Veritau in 2017/18.

APPENDIX 1 – ACTIONS AGREED TO ADDRESS CONTROL WEAKNESSES

Action Number	Report Reference	Issue	Risk	Agreed Action	Priority*	Responsible Officer	Timescale
1	2.1	Changes to the requirements of the standard, or in systems and processes subject to the standard, may not be recognised and acted upon.	Non-compliance with the PCI DSS, leading to the imposition of fines, increased transaction charges, or suspension of ability to process card payments.	See 5.1 above.	2	Financial Transactions Manager (Corporate Accountancy)	30/04/2017 for initial steps, with full work to follow in due course.
2	2.2	The council has not documented and assessed for compliance all processes which may be subject to PCI DSS requirements.	Non-compliance with the PCI DSS, leading to the imposition of fines, increased transaction charges, or suspension of ability to process card	See 5.2 above.	2	Financial Transactions Manager (Corporate Accountancy)	30/04/2017 for initial steps, with full work to follow in due course.

			payments.				
3	2.3	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.	Non-compliance with the PCI DSS, leading to the imposition of fines, increased transaction charges, or suspension of ability to process card payments.	See 5.3 above.	2	Financial Transactions Manager (Corporate Accountancy)	30/04/2017 for initial steps, with full work to follow in due course.
4	2.4	Although the standard states "Merchants and service providers must manage and monitor the PCI DSS compliance of all associated third party service providers with access to cardholder data", the council has not fully established	Equipment, systems or web links may be manipulated, leading to fraud or cardholder data being compromised, imposition of fines, increased transaction charges, or	See 5.4 above.	2	Financial Transactions Manager (Corporate Accountancy)	30/04/2017 for initial steps, with full work to follow in due course.

		who is responsible for maintaining the integrity of payment methods.	suspension of ability to process card payments.				
5	2.5	Self-assessment questionnaires may not have been completed and submitted for all payment channels.	Non-compliance with PCI DSS, leading to the imposition of fines, increased transaction charges, or suspension of ability to process card payments.	See 5.5 above.	2	Financial Transactions Manager (Corporate Accountancy)	30/04/2017 for initial steps, with full work to follow in due course.

*The priorities for actions are:

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.