

Swindon Internal Audit Services

Chief Executive's

Strictly Private and Confidential

Payment Card Industry Standards

Report status: Final

Report date: 29th July 2010

Report Reference: Finance/PCIS/DS

Auditor: Dawn Sexstone, CIPFA Trainee

Issued by: Nikki Soave, Principal Auditor

Contents	Page
Section 1 Executive Summary	3
Section 2 Introduction	4
Section 3 Approach	4
Section 4 Risk Areas Examined	5
Section 5 Overall Opinion	5
Section 6 Secure Procedures	7
Section 7 Acknowledgement	7
Section 8 Action Plan	8

Appendices:

A: Standard Audit Opinions

Report distribution:

Draft for discussion issued: 7th June 2010

Paul Smith Group Finance Manager - Technical

Final issued: 29th July 2010

Paul Smith Group Finance Manager - Technical

Fiona Pearce CAPITA - Head of Finance Administration

Anna Marzec Data Protection Officer

Stuart McKellar Director of Finance

1 Executive Summary

- 1.1 This audit has been undertaken as part of the audit plan and included a follow up on previous audit recommendations made in the Payment Card Industry Data Security Standards audit in December 2008.
- 1.2 The aim of the audit was to look at the current controls and processes in place across the Council and to give an audit opinion on whether the controls are adequate enough to comply with the Payment Card Industry Standards.
- 1.3 The areas being covered in this audit are departments which receive and process their own credit /debit card payments and departments which receive telephone payment requests that are passed on to a third party department for processing. The audit did not cover the IT and network security side of the Payment Card Industry Standards.
- 1.4 The main findings were that there had been no significant improvements made to comply with the Payment Card Industry Standards since the previous audit conducted in 2008/09. A project had been put together to address the issues of PCI compliance but the project was put on hold due to the issues around IT requirements which arose after project inception. As a result there are still areas that have not received any training in the Payment Card Industry Standards on what is expected of staff either in their role as a payment processor, or for those receiving payment details over the telephone.
- 1.5 Across the different sites the following key issues were found:
 - Cardholder's security codes were being kept.
 - Some departments had not received Payment Card Industry Standards training.
 - Storage of cardholder information was not consistent across the Council.
- 1.6 The key recommendations from the report are:
 - The re-programming of all credit/debit card payment devices to ensure that the full 16-digit card number is no longer printed on the Merchant copy receipt.
 - Clarification should be provided by Corporate Finance to advise the correct length of time that credit/debit card receipts should be retained and then communicated to all departments.
 - Review of processing procedures to ensure that under no circumstance the cardholder's security number is retained on any paperwork being held as this is in breach of the Payment Card Industry Standards.
- 1.7 The result of the audit testing in relation to compliance with the Payment Card Industry Standards indicated that significant improvements were required. The system was defined as one of high materiality and impact and therefore combining this with the opinion on internal controls gives an overall rating of the audit was **of concern**.

2 Introduction

- 2.1 An internal audit review of the existing processes in place with regards to the receiving of Credit and Debit card payments was carried out as part of the agreed Audit Plan. This is intended to provide assurance to the Director of Finance that the systems of internal control are operating adequately and effectively.
- 2.2 Across the Council there are a number of sites and departments which either directly receives payments, or who receive cardholder data for processing by another department. The process of receiving debit and credit card payments should comply with the Payment Card Industry Standards and any areas of non-compliance should be identified and corrected.
- 2.3 There are three main processes being used to receive debit and credit card payments, they are as follows:
- Chip and pin devices – the payment device is directly connect to the Bank by its own telephone line and payments can be processed using chip and pin, by swiping the card and obtaining a signature, or as a cardholder-not-present transaction.
 - AXIS Counter Receipting – this is a computer software package that can be used either with, or without, a PDQ machine. The payment details are input into the system that records the transaction value, if the cardholder is present then the PDQ machine is used to authorise the payment. If the cardholder is not present then payments are processed through Capita Finance and a PDQ machine is not required.
 - Flex system – this is the swipe card system being used at all the Recreation sites and again is a software package linked to a swipe card device and requires the card holder to sign the merchant copy of the receipt.

3 Approach

- 3.1 Managers determine the extent of internal control in their systems and are responsible for providing an environment that ensures that resources are properly applied, value for money is secured, fraud and other losses prevented, and the Council's Financial Regulations are complied with.
- 3.2 Internal Audit, as a service to the Directorate and the Council as a whole, contributes to internal control by examining and evaluating its adequacy and effectiveness. The auditor's responsibility is to form an independent opinion, based on the audit work undertaken, on the reliability of the systems of internal control, risk management and governance, reviewed and report this to the Director of Finance and to other relevant Managers.
- 3.3 In accordance with best practice, a risk-based approach was adopted that identified the key risks to the business objectives and those mitigating actions/controls that should be in place. The auditor then assessed the effectiveness of the mitigating controls through examination of relevant documents, procedures and detailed testing.

- 3.4 The appropriate managers and staff were consulted during the course of the review and examination and testing of relevant documentation and procedures took place within departments.

4 Risk Areas Examined

- 4.1 The key risks to the achievement of the business objectives were agreed with the Director of Finance before the commencement of the audit. The table below summarises the Risk Areas examined during the review and provides an assessment of the adequacy of the mitigating controls in place for each area of risk examined:

Risk Area Examined	Audit Conclusion re. mitigating controls
<ul style="list-style-type: none">Financial Loss to the Authority	Significant improvements required
<ul style="list-style-type: none">Identity theft or Fraud	Significant improvements required

5 Overall Opinion

- 5.1 **Materiality and impact: High.** In the worst-case scenario, failure to comply with the PCI/DSS risks disclosure, modification and/or deletion of customer data further placing at risk the integrity (accuracy and completeness) of the Council's financial records and accounts. The maintenance of privacy and security is a statutory requirement. Non-compliance with the legislation will place the Council at risk of prosecution through the Courts, loss of public confidence and political embarrassment. Ultimately the cardholder may be placed at risk of "identity theft" and financial loss. The political, social and financial repercussions potentially arising from inadequate control determines the classification of **high materiality** and **impact** for this environment.
- 5.2 **Opinion on system controls: Significant improvements required** (see Appendix A) i.e. the auditor completing the review concluded that existing procedures needed to be improved to ensure that they are fully reliable. A number of significant recommendations have been made to improve missing or failing controls.
- 5.3 **Overall assessment of risk:** the combination of the high impact of the system, along with the opinion on the system controls gives an overall risk assessment to the Council as being **of concern**:

		MATERIALITY AND IMPACT		
SYSTEM CONTROL		High	Medium	Low
1	High standard	Moderate	Minimal	Minimal
2	Satisfactory	Moderate	Moderate	Minimal
3	Significant Improvements required	Of Concern	Moderate	Moderate
4	Fundamental weaknesses identified	Significant	Of Concern	Moderate

- 5.4 The following key recommendations should be implemented in order to achieve the improvements required:
- The re-programming of all credit/debit card payment devices to ensure that the full 16-digit card number is no longer printed on the Merchant copy receipt.
 - Clarification should be provided by Corporate Finance to advise the correct length of time that credit/debit card receipts should be retained and then communicated to all departments.
 - Review of processing procedures to ensure that under no circumstance the cardholder's security number is retained on any paperwork being held as this is in breach of the Payment Card Industry Standards.
- 5.5 Management's response to the Internal Audit recommendations is included in the action plan at section 8 of the report on completion of the audit.
- 5.6 All of the matters arising are detailed in the action plan, together with suitable recommendations, together with an indication as to whether the matters arising are of a high, medium or low priority. The action plan provides a checklist of the findings of the review, potential consequences, and identifies officers responsible for implementing the recommendations and appropriate time-scales.

6 Secure Procedures

- 6.1 It was noted that the following secure procedures are now an integral part of the Payment Card Industry Standards system:
- The Cashier's process for receiving cardholder present payments is robust and the system being used is functioning effectively.
 - All new cashiers are made fully aware of the Payment Card Industry standards and sign to confirm that they have read the standards.

7 Acknowledgement

- 7.1 Internal Audit would like to acknowledge and thank the following Officers who contributed to the review:

Name	Job title
Paul Smith	Group Finance Manager - Technical
Sheila Jennings	Admin Assistant - Enterprise Works
Marilyn O'Sullivan	Receptionist - Registrar Office
Caroline Lovett	Duty Manager - Steam Museum
Mike Crossland	Duty Manager - Steam Museum
Janice Leard	Information Centre Manager
Gail Midwinter	Capita Finance - WTW1
Freida Savage	Capita Finance - WTW1
Nicki Western	Culture Marketing Manager - Arts Centre
Fiona Page	Community Facilities Business Support Officer
Roxanne De'Lecia	Revenues Officer - Credit Control
Lee Haines	Processing Clerk - Parking Admin
Mary Turner	Senior Cashier
Liz Burton	Building Control Officer

Section 8: Action Plan

The purpose of this action plan is to provide a summary of the matters arising during the audit of Payment Card Industry Standards, together with the recommendations to mitigate risks, the manager's response to the recommendations, along with the officer responsible and timescale for implementation. In order for you to identify the most significant matters arising, which affect the reliance that can be placed on the controls reviewed, the recommendations have been prioritised.

Ref.	Finding	Recommendations Priority (High/Medium/Low)	Responsible Officer and Timescale	Management Response
1	Risk: Identity and Financial Theft - Corporate Policies and Procedures			
1.1	The latest Retention and Disposal Policy available on the Council's Intranet pages was issued in May 2005. On reviewing this document it was found that there is no specific entry for the retention and disposal of Credit and debit card receipts.	<p>The current Retention and Disposal policy should be updated to include the length of time credit/debit card receipts should be retained and how they should be disposed off for both chip and pin, and non chip and pin transactions.</p> <p>Priority: Medium</p>	<p>Data Protection Officer</p> <p>August 2010</p>	This will be updated as part of the re-continuation of the PCI compliance project. This area can be targeted for immediate update.

Final Internal Audit Report – Payment Card Industry Standards

Ref.	Finding	Recommendations Priority (High/Medium/Low)	Responsible Officer and Timescale	Management Response
2	Risk: Identity and Financial Theft - Testing of sites with payment card facilities.			
2.1	<p>Testing was undertaken on the following seven Council run sites that have there own card payment facilities:</p> <ul style="list-style-type: none"> • Enterprise Works • Registrar Office • Steam • Premier House, Reception • Information Centre • Capita Finance • Arts Centre <p>It was found that they were all producing merchant receipts that showed the full 16-digit card number.</p> <p>This is in breach of the Payment Card Industry standards (3.3), which state that the full card number (PAN) should only be displayed in full if there is a legitimate business needs to see the full PAN.</p>	<p>All debit/credit card machines should be re-programmed to comply with the PCI guidance that only the first 6 and last 4 digits should be visible as a maximum.</p> <p>Priority: High</p>	<p>Group Finance Manager - Technical</p> <p>August 2010</p>	Agree

Final Internal Audit Report – Payment Card Industry Standards

Ref.	Finding	Recommendations Priority (High/Medium/Low)	Responsible Officer and Timescale	Management Response
2	Risk: Identity and Financial Theft - Testing of sites with payment card facilities.			
2.2	<p><u>Enterprise Works</u> During testing of PCI compliance at Enterprise Works it was found that the receipts are stored in cardboard archive boxes in the archive room. The Archive room does not get locked up and the boxes are not kept in a lockable cupboard.</p> <p>This is in breach of the Payment Card Industry standards (9.6), which states that they need to physically secure all papers that contain cardholder data.</p>	<p>All receipts should be held securely to prevent unauthorised access to confidential information.</p> <p>Priority: Medium</p>	<p>General Manager – Enterprise Works</p> <p>August 2010</p>	Agreed – will be taken up with the Enterprise Works Manager
2.3	<p><u>Steam Museum</u> During PCI compliance testing at Steam it was found that they are holding financial information, which goes back since the site opened 10 years ago. This is in breach of the Council's Data Retention and disposal policy, which states financial information should be held for 7 years.</p>	<p>Clarification should be provided by Corporate Finance to advise the correct length of time that credit/debit card receipts should be retained and then communicated to all departments.</p> <p>Records held that are over 7 years old should be disposed of securely.</p> <p>Priority: High</p>	<p>Group Finance Manager - Technical</p> <p>August 2010</p> <p>General Manager – STEAM</p> <p>August 2010</p>	Agreed

Final Internal Audit Report – Payment Card Industry Standards

Ref.	Finding	Recommendations Priority (High/Medium/Low)	Responsible Officer and Timescale	Management Response
2	Risk: Identity and Financial Theft - Testing of sites with payment card facilities.			
2.4	<p><u>Information Centre</u> The Information Centre processes payments both over the telephone and when the cardholder is present. It was found that the Telephone Payment Request sheets that are used to record the payment details received over the telephone, are being kept for 6 to 12 months before disposal.</p>	<p>Telephone Payment Request sheets should be disposed of promptly and securely once the transaction has been processed electronically.</p>	<p>Information Centre Manager</p> <p>August 2010</p>	<p>Response by J Leard, Visitor Information Centre Manager</p> <p>As soon as the transaction has been processed the Telephone Payment Request sheets are promptly held in the safe, which is only accessible by the responsible key holders. After a period of 6 months they are shredded by a cross-shredder. They are kept for a period of 6 months, as this is a requirement in case of charge-backs.</p>
2.5	<p><u>Information Centre</u> The Telephone Payment Request sheet being used by the Information Centre to record telephone payments was found to include the cardholders' 3-digit card security number. These forms are then kept for 6 to 12 months in their safe.</p> <p>This is in breach of the Payment Card Industry standard (3.2.2), which states that the card verification code or value used to verify 'card not present' transactions should not be stored.</p>	<p>Cardholder's security codes should not be kept once payment has been processed, as this is in breach of PCI requirements.</p> <p>Priority: High</p>	<p>Information Centre Manager</p> <p>August 2010</p>	<p>Response by J Leard, Visitor Information Centre Manager</p> <p>We will promptly devise a system whereby the 3-digit card security number is not recorded on the Telephone Payment Request sheet and once the transaction is processed the security number will be destroyed.</p>

Final Internal Audit Report – Payment Card Industry Standards

Ref.	Finding	Recommendations Priority (High/Medium/Low)	Responsible Officer and Timescale	Management Response
2	Risk: Identity and Financial Theft - Testing of sites with payment card facilities.			
2.6	<p><u>Capita Finance</u></p> <p>The AXIS system being used by Capita Finance allows the processing of card payments without the need for the 3-digit security code or any other security checks being undertaken.</p> <p>This increases the chance of fraudulent payment information being processed by the Council.</p>	<p>The Council should introduce an additional security check to mitigate the chances of fraudulent payments being made to the Council.</p> <p>Priority: High</p>	<p>Group Finance Manager - Technical</p> <p>August 2010</p>	<p>'For cardholder present transactions 'chip and pin' machines are to be used. The security number is not required for these transactions. For transactions where the cardholder is not present, the introduction of the paye.net system later in 2010 will allow for security card numbers to be taken. The use of these will be considered during its implementation. The Axis system does not have a 'field' for security numbers.'</p>

Final Internal Audit Report – Payment Card Industry Standards

Ref.	Finding	Recommendations Priority (High/Medium/Low)	Responsible Officer and Timescale	Management Response
3	Risk: Identity and Financial Theft - Testing of departments taking payment information over the telephone.			
3.1	<p><u>Community Hire</u></p> <p>When Community Hire take payments over the telephone they are currently recording the 3-digit security code on the telephone request forms, as it is required in order to process the payment at Premier House.</p> <p>The retaining of the security verification number is in breach of the Payment Card Industry standards (3.2.2) that states: 'do not store the card-verification code or value used to verify card-not-present transactions'.</p> <p>The Community Hire team will be moving to WTW5 in April 2010 and once they have moved their payment requests will be sent to Capita Finance (WTW1) for processing and the need to record this information will change. Once Capita Finance has processed the payment all the paperwork will be held in the Cashiers department and they will be responsible for the disposal of the forms.</p> <p><u>Building Control</u></p> <p>Testing established that although Building Control do not ask the Cardholder for the security code occasionally they may be given this information by the cardholder which they record on the Telephone payment request form.</p>	<p>The 3-digit security code should not be retained once processing has been undertaken, this information should be removed from any forms being held within the departments.</p> <p>Priority: High</p>	<p>Head of Finance Admin (Capita)</p> <p>August 2010</p>	Agreed

Final Internal Audit Report – Payment Card Industry Standards

Ref.	Finding	Recommendations Priority (High/Medium/Low)	Responsible Officer and Timescale	Management Response
3	Risk: Identity and Financial Theft - Testing of departments taking payment information over the telephone.			
3.2	<p><u>Credit Control</u> The Credit control team were due to receive training for PCI compliance but the PCI DSS Compliance project got put on hold before they had received the training.</p> <p><u>Parking Services (BSU)</u> During the testing it was established that the team had not received any training on PCI compliance.</p> <p><u>Building Control</u> During the testing it was established that the team had not received any training on PCI compliance.</p> <p>Anyone receiving payment information over the telephone should be made aware of the Payment Card Industry standards, as they are applicable to the role the employee is undertaking. Lack of awareness will lead to errors being made and data being stored incorrectly.</p>	<p>Any employee responsible for taking credit/debit card payments over the telephone should be aware of the Payment Card Industry standards and be advised on the issue of best practice.</p> <p>Priority: Medium</p>	<p>Group Finance Manager - Technical</p> <p>August 2010</p>	<p>All employees identified as responsible for taking payments were identified and invited to attend general PCI training, which includes some of the sections highlighted at 3.2</p> <p>Training will again be undertaken as part of the restart of the PCI project.</p>

Final Internal Audit Report – Payment Card Industry Standards

Ref.	Finding	Recommendations Priority (High/Medium/Low)	Responsible Officer and Timescale	Management Response
3	Risk: Identity and Financial Theft - Testing of departments taking payment information over the telephone.			
3.3	<u>Parking Services (BSU)</u> The form being sent to Capita Finance for processing includes the 3-digit security code from the back of the card, other departments sending payments through WTW1 do not record this information.	Procedures need to be introduced to ensure all departments are aware of their responsibilities and that the practice of receiving payment card information over the telephone is consistent across the Council. Priority: High	Group Finance Manager - Technical August 2010	Response by F Pearce Responsibility for reconciliation of TIC cash / card takings is the responsibility of Capita Finance Admin therefore we have to have the merchant copies. I would question this recommendation as the storage of merchant copies in central finance admin is more secure than TIC and does not negatively impact procedures, policy or security. Introducing Paye.net will address this issue.
4	Risk: Financial loss to the Authority			
4.2	The contract did not contain a list of the establishments that were included. The information which was provided for tender was the total number of transactions – <ul style="list-style-type: none"> • Credit Card payments – volume 36,975 transactions at a value of £1,380,185. • Debit Card payments – volume 121,580 transactions with a value of £4,767,355. The description of the service within the tender was 'The processing of credit and debit card transactions at various locations'.	A list of sites included should be held with the contract and kept up to date, new sites should be added when identified as requiring this service. Priority: Medium	Group Finance Manager - Technical August 2010	Unclear what the purpose of this recommendation is and what advantages this would bring.

Standard Audit Opinions

1. The audit opinion is based on two different criteria the first is the materiality of the system and it's impact on the Council if there was a system failure. This has been spilt into High, Medium or Low.
2. The second criteria, is the standard of control found within the system audited. This has been categorised into 4 different levels i.e. high; satisfactory; significant improvements required and, fundamental weakness. Each of these categories has a standard opinion (see below).

Standard Audit Opinions on System Control

Audit Opinion 1. *High Standard*

The auditor completing the review concluded the significant system controls are in place and operating effectively and only minor recommendations have been made.

Audit Opinion 2. *Satisfactory Standard*

The auditor completing the review concluded that most of the significant controls are in place and operating satisfactorily although some non-compliance was identified and therefore there is scope for improvement.

Audit Opinion 3. *Significant Improvements Required*

The auditor completing the review concluded that existing procedures needed to be improved to ensure that they are fully reliable. A number of significant recommendations have been made to improve missing or failing controls.

Audit Opinion 4. *Fundamental Weaknesses Identified*

The auditor completing the review concluded that the matters arising from the review are sufficiently significant to place doubt on the reliability of the procedures reviewed. Implementation of the recommendations made is a priority to ensure that reliance can be placed on the system.

3. The combination of these two factors gives an overall risk assessment to the Council of one of four scores i.e. significant, of concern, moderate or minimal (see section 4 of the main report).