INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Payment Card Industry – Data Security Standard
TO:	Chief Executive	**DATE:**	30 March 2015
C.C.	Head of Finance ICT Services Manager Customer Contact Manager Applications Support Manager		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2014/15, an examination of the above subject area has been undertaken and this report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 This topic has not been audited directly before, although it formed part of a piece of consultancy work performed by the council's previous ICT Audit contractors. Certain aspects are also covered during audits of establishments where payments are taken.

1.3 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

2 Background

2.1 The Payment Card Industry Data Security Standard (PCI DSS) is mandated by the main card issuing companies (e.g. Visa, MasterCard, American Express etc.). This standard is an amalgamation of the standards that each company previously had in place.

2.2 The aim of the standard is to help organisations proactively protect customer card data including PIN numbers and personal data held on the cards. The scope of the standard includes all of the ICT inventory which deals with the data, including any networks that the data may cross, and the physical security of the locations taking the payments.

2.3 Non-compliance with the standard can lead to fines being levied and possibly the suspension of card payment acceptance.

2.4 As the council has not yet completed the relevant self-assessments to show compliance, fines are being imposed on a monthly basis by Global Payments (formerly part of HSBC), with total fines for the current financial year being in the region of £10,000.

3 Scope and Objectives of the Audit

3.1 The audit was undertaken to look at the approach that has been taken with regards to achieving PCI DSS compliance and the steps that still need to be taken. This included the methods used in securing the card payments and details taken by the Customer Services Centre at Warwickshire County Council on our behalf and payments taken at the various Cultural Services facilities.

3.2 In terms of scope, the audit covered the following areas:

- Project planning and review
- Customer Service Centre
- Leisure centres
- Royal Spa Centre and Town Hall.

3.3 The audit programme identified the expected controls. The control objectives examined were:

- The council has a clear plan in order to achieve compliance with the standard.
- Progress against the project plan is communicated appropriately to relevant staff.
- The council will be better placed to undertake projects of this nature in the future.
- Payments can be taken on our behalf by the Customer Service Centre at Warwickshire County Council.
- Card payments taken at the council's leisure centres are PCI DSS compliant.
- Card payments taken at the Royal Spa Centre and Town Hall are PCI DSS compliant.

4 Findings

4.1 Project Planning & Review

4.1.1 A project brief was drawn up at the start of the project in November 2012. It was agreed by SMT prior to the formal commencement of the project that the council would only use standalone PDQ machines in order to remove the network from the compliance scope. A project initiation document and project plan documents were then drawn up.

4.1.2 The Application Support Manager (ASM) advised at the start of the audit that this plan not been adhered to, with changes to the timescales and individual aspects being required. As at the time of the audit, the project is still not complete.

4.1.3 A chronology spreadsheet produced by the ASM provided links to numerous emails and documents which highlighted that relevant staff and project board members were being provided with regular updates as to the progress with the project.

4.1.4 A project site is being maintained on the intranet and, as part of this, the ASM has produced a number of different records including logs of issues encountered during the project, lessons to be learnt and recommendations with regards to how the council maintains compliance once it has been achieved.

4.1.5 The ASM advised that the main issue holding up completion of the project is that a compliant solution is still awaited from BT for the Royal Spa Centre (RSC) / Town Hall box office. She advised that BT are being chased, but there is no current completion timescale. Consideration is also being given to changing the ticketing used at the box office, so this could also have an impact on the completion of the project (see 4.4 below).

4.1.6 The final step, prior to the completion of the relevant self-assessment questionnaires (SAQs), will be to ensure that all relevant staff have received training. This will include staff at the Art Gallery & Museum (AGM), where standalone PDQs have always been in use (and were, therefore, not included in the project).

4.1.7 Staff at the Althorpe Enterprise Hub will not, however, require training, as it was decided in the early stages of the project that they would no longer take card payments.

4.1.8 As some strands of the project are complete, a query was raised with the ASM as to whether site-specific assessments were an option, so as to reduce the amount of fines being levied.

4.1.9 The ASM advised that the council is associated with two acquiring banks, with the council's PDQ payments going to HSBC and the Customer Service Centre (CSC) payments going to RBS.

4.1.10 Separate SAQs are required by each acquiring bank and the council could, therefore, complete the RBS SAQ now, as the council can show compliance for the CSC (see 4.2 below). However, RBS are not currently imposing any fines.

4.1.11 She also advised that, whilst the leisure centres (see 4.3) and the AGM are compliant, once all training can be verified, we cannot complete the SAQ for HSBC until all relevant sites are compliant, so the council has to wait until the RSC telephony issue has been resolved before this can be completed.

4.2 Customer Service Centre

4.2.1 When the compliance project started, there were four council PCs in the CSC on which payments to the council could be taken. These PCs were operated by council staff. They were on a dedicated council network and passed through the council's firewall, so were in scope in terms of the council's PCI DSS compliance.

4.2.2 Copies of various email exchanges between staff at each council were provided which set out how the process would be changed to a service provider model, with all of the associated cardholder data functions being outsourced to Warwickshire County Council (WCC).

4.2.3 The payments are now being taken on WCC PCs (with no council machines being in place) by any available staff member and the details do not cross our network. The more recent emails highlighted that testing has been undertaken by WCC to confirm that the payment icons for the new processes are working and the relevant network connections could be removed. Therefore, the payments taken at the CSC are now outside of the scope of the council's 'physical' PCI DSS compliance.

4.2.4 A formal agreement is now in place with WCC for them to provide PCI DSS compliant card payment services on the council's behalf. Section six of the agreement highlights that WCC will ensure that its ICT systems and technology, processes, data security controls and data flows used in the CSC will be compliant with the standard and that, from 1 April 2015, a certificate of its compliance will be held.

4.2.5 The ASM advised that the consultant from Dionach, who has been providing advice to the council on achieving compliance, has advised that it is acceptable for the council to complete its compliance assessments in the knowledge that WCC is working towards compliance.

4.2.6 This was assuming that the agreement was in place and that there is a document which sets out which requirements will be managed by them and which will remain the responsibility of the council. The ASM confirmed that this will be in place.

4.2.7 Upon review of the email exchanges, it was also highlighted that some staff at the CSC had received training on the new processes and more was planned. A copy of the training questionnaire that had been produced by the Warwickshire Direct Trainer at WCC was provided and this was considered to be appropriate.

4.3 Leisure Centres

4.3.1 At the start of the project, some of the leisure centres were using VoIP (Voice over Internet Protocol) phones and the others had analogue lines, with the PDQ machines being connected to the FLEX system so that the payments were automatically calculated based on the services being purchased as per FLEX. This meant that the card data was crossing the network, bringing the whole network into the scope of PCI DSS.

4.3.2 Consideration was given to segmenting the network, so that only part of it was in scope. However, it was subsequently decided that the network link would be removed and that analogue phone lines would be in place for all PDQ machines, with the link to the FLEX system being removed.

4.3.3 Links to various email exchanges and other supporting documents were held on the chronology spreadsheet which set out how this solution was agreed and implemented. The system is now in place as described above.

4.3.4 The ICT Trainer provided a copy of the course slides for the training that had been set up for those who are to take card payments at the council. These gave details of what PCI DSS is, why it is relevant, who it applies to and what staff need to do in order to maintain compliance.

4.3.5 An email had been received from the Sports Facilities Area Manager (SFAM) confirming that, with the exception of some casual staff, all relevant staff had undertaken the training. The casual staff would be trained as and when they asked for work.

4.3.6 The four main leisure centres were visited during the course of the audit and the staff on reception at each venue were spoken with. Each confirmed that they had received the training, with one staff member having a paper copy of the slides to hand.

4.3.7 One aspect of compliance with the standard requires the card data to be physically secure and, in a practical sense, this means that the full card number (PAN numbers) should not be displayed on the copies of the card receipts held by the council (the merchant copies). As the PDQ machines held do not redact the numbers automatically, the numbers have to be obscured by pen.

4.3.8 At three of the four sites, the PAN numbers on the card receipts held for the shift had not been redacted. In each case, the staff member concerned advised that they had been too busy to do them at the time, as swimming lesson enrolments were being dealt with. In most cases the staff advised that, when redactions were being performed, they were redacting part of the PAN numbers as suggested by the training, but one was redacting the whole number and expiry dates.

4.3.9 They all advised that the receipts were not being retained after the end of each shift, as summary figures were obtained from the PDQ machines. They also all confirmed that the receipts would be cross-shredded.

4.3.10 The SFAM advised that the shredding at the end of each shift had been a management decision to ensure that any receipts that had not been redacted at the time of the payment were destroyed at the earliest opportunity.

4.3.11 Staff at each site also confirmed that they were aware of the need to keep all personal belongings out of the payment area, with each advising that lockers were available. However, at one site, a handbag was in the reception area and the staff member concerned acknowledged that this should not have happened.

4.3.12 As highlighted above, the PDQ machines are no longer connected to the FLEX system, and the manual entry of figures to the PDQ machines was observed at each site where a card payment was received during the visit.

4.4 Royal Spa Centre & Town Hall

4.4.1 The situation at the RSC and Town Hall had been complicated by the fact that payments could be taken at either site. An email identified on the chronology spreadsheet highlighted that various solutions had been examined to try to retain some of this functionality, but it has been decided to move all payment calls to one site (Town Hall) with details going over an analogue phone line with no information going over the network.

4.4.2 However, as suggested above, there is still no telephony solution as the box office needs to allow calls to be queued and for marketing messages to be played, so this aspect of the project remains incomplete.

4.4.3 As also previously highlighted, a further complication may be brought about by the proposed change from the current ticketing system (Data Box). The ASM advised that a conference call is due to be held with the company that sells the proposed new system and aspects of PCI DSS compliance will be covered during this discussion.

4.4.4 The email from the SFAM (see 4.3.5 above) also included details of staff from the RSC and Town Hall who had taken the training as at that point in time. Upon review of the intranet staff directory a further eight staff members from the RSC and Town Hall were identified who were not included on the list.

4.4.5 Upon discussion with staff at the RSC during a site visit, it was confirmed that those staff that required training (i.e. those who may have access to the card data) had taken it, but some technical staff would not need to do it.

4.4.6 No specific testing on compliance with the relevant aspects of the training was performed at the RSC or Town Hall. However, it was noted that an issue regarding the redaction of PAN numbers was raised during a specific, recent, audit of the RSC and it was confirmed by staff that they were aware of the instruction to redact the numbers and confirmed that it was now being carried out as appropriate.

5 Summary & Conclusion

5.1 Following our review, we are able to give a SUBSTANTIAL degree of assurance that the processes being adopted to ensure compliance with the Payment Card Industry Data Security Standard are appropriate.

5.2 No formal recommendations are included in the report, as relevant staff are aware of the steps that are still required for compliance to be achieved (notably the introduction of a compliant solution for the Royal Spa Centre box office and the completion of the relevant self-assessments) and lessons to be learnt from the project have been identified by them. It is, however, felt worth reiterating that fines are currently being imposed, so efforts should be made to ensure that the project is completed at the earliest possible opportunity.

Richard Barr
Audit and Risk Manager