Payment Card Industry – Data Security Standards

November 2019

Low Assurance

Lisa Lovegrove CMIIA, CISA, Chief Internal Auditor
Denbighshire Internal Audit Services, Caledfryn, Smithfield Road, Denbigh, LL16 3RJ

Lisa Lovegrove CMIIA, CISA, Chief Internal Auditor
Denbighshire Internal Audit Services, Caledfryn, Smithfield Road, Denbigh, LL16 3RJ

Background

The Payment Card Industry Data Security Standards (PCI DSS) is an information security standard for organisations that handle credit card payments. The standard was created to increase controls to protect cardholder data and to reduce credit card fraud. Any cardholder data breach would be seen as a failure to protect personal data and potentially attract monetary penalties under General Data Protection Regulations (GDPR) and could even mean barring from accepting card payments in future.

Compliance with this standard is not a legal requirement; however, card merchants and software suppliers may ask for compliance as part of their contract or agreement. The standard requires testing of IT connections and certification that staff have had training with regard to card usage, storing and disposal of card information.

Purpose & Scope of Review

We carried out a review of compliance with PCI DSS requirements and to provide assurance for the Section 151 Officer, Senior Management and inform the Annual Internal Audit Report and Annual Governance Statement.

The review focused on the following areas:

- Roles and responsibilities;
- Policy and procedures;
- Training and awareness
- Payment Card Environment;
- Processing card payment data;
- Third party processors' compliance; and
- Compliance testing and self-assessment.

Audit Opinion

Overall, our testing confirms that not all services taking card payments on behalf of the council can demonstrate that they fulfil the requirements of the standards.

Finance and ICT are aware that there are weaknesses and standards are not being met across all areas. Cross-service involvement is required to achieve compliance, but overall responsibility to develop a strategy or programme has not been assigned to ensure that suitable arrangements are in place corporately i.e. coordinating a self-assessment, accreditation, training, ICT security (Risk issue 1).

The Information Security Policy covers Chip and Pin and the council's response should there be a data security breach involving card data. However, it does not reference the need to comply with the PCI DSS or guidance as to how this would be achieved. (Risk Issue 3)

There is a lack of consistency regarding training to ensure that staff are suitably aware of how to handle card payments securely, with several departments adopting a 'common sense' or informal approach. The departments with the largest volume of staff taking card payments have records to evidence the training that has been given (for instance, Leisure services and Customer services). (Risk issue 2).

Several services are able to take card payments in person, on the phone or online. The standards require that lines carrying card data are tested quarterly, including those that go through our firewalls, to verify that they are secure. These lines are a means of transferring the information and, for very short periods of time, when portals are open they could be vulnerable to a cyber-attack. The majority of card payment traffic is through the council's internet and firewalls, but some use:

- A direct phone line dial-up connection that is outside the council's firewalls.
- A SIM card to transfer data.

Currently, only payments administered by Capita (which includes payments taken by the cash office, contact centre and some other services areas) and the provider for Café R (Payment Sense) are compliant with this requirement.

There are several agreements with one card service provider (Worldpay), which has resulted in different levels of charges. This includes small penalty charges as two card payment terminals are not compliant (both terminals need upgrading to avoid future penalties). The Business and Risk Manager has tried to bring all the agreements under one charging structure to aid administration and obtain value for money, but, so far, he has been unable to gain the agreement of the provider. (See Risk Issue 4)

The council has agreements with several other card service providers due to:

- Software systems compatibility;
- Services involve ICT and procurement too late to explore the possibility of using an existing provider, and
- Urgency to finalise an agreement so as not to cause delay to a project completion date (Links to Risk Issue 5)

These providers are not currently charging penalties for non-compliance.

Corporately, there is little oversight of the multiple agreements in place making the card environment more complex than it needs to be. This raises the risk of security vulnerabilities going undetected (Risk issue 4)

The council should also be ensuring that its external service providers are compliant with these standards, but there was no evidence that this was requested when agreements were being formed.

The council has signed a declaration with one supplier where the council confirmed that it is compliant with the standards. Also, a pay by phone contract with one supplier is currently being extended. To use the supplier's pay by phone function, the card details must be pre-registered, but the contract with makes no mention of:

- Length of time such data is retained;
- Supplier's compliance with PCI DSS; nor
- Secure disposal of any card data once the contract is ended.

We raise a risk issue to ensure that procurement and contracts consider PCI-DSS requirements and that suitable checks are carried out to verify that card payment data processed on the council's behalf is managed in accordance with the standards (Risk Issue 5).

While there are areas of good practice, we give a low assurance rating due to the nature of the issues and control weaknesses identified. Co-operation across all services is required to drive this forward to ensure that the council meets the required standards.

Low assurance	Significant weaknesses in management of risks and/or controls that put achievement of objectives at risk.

Action Plan

Audit Review of: PCI DSS

Date: November 2019

Corporate Risk/Issue Severity Key	
0	**Critical** – Significant issues to be brought to the attention of SLT, CET, Cabinet Lead Members and Corporate Governance Committee
2	**Major** – Corporate, strategic and/or cross-service issues potentially requiring wider discussion at SLT and/or CET
3	**Moderate** – Operational issues that are containable at service level

Risk Issue 1	**The council does not have a programme or strategy in place to ensure corporate compliance with PCI-DSS. This poses the risk of financial and/or reputation loss and potential withdrawal from payment card acceptance programmes.**		
Background Detail	There is no formal plan or programme which is regularly reviewed/updated to ensure compliance with PCI-DSS. This is compounded by the fact that responsibility for taking this forward corporately has not been assigned to ensure that all services that take card payments are compliant. Once responsibility is assigned, the programme should comprise of: • An annual PCI-DSS attestation of compliance along with completion of a self-assessment questionnaire; • Production of a map of the card environment to show the type of transactions and where they are taken; • Quarterly network scans by an approved scanning vendor in accordance with PCI-DSS.		
Action (Ref)	**Agreed Management Action**	**Responsibility**	**Deadline**
1.1	Report to SLT to ensure corporate buy-in.	Chief Accountant / Chief Internal Auditor	31/12/2019
1.2	A cross disciplinary Task and Finish Group/Project team will be set up to implement the changes required. The Key services that need to be included in the T&FG include: • Finance • ICT • Information Management • Customer Services	Business and Risk Manager	31/12/2019

	• Procurement Service • Service / User Group Representation.		
1.3	The T&FG will devise a programme which will take account of the issues raised. It is vital that SLT have input into and buy-into the programme as it will impact a number of services. This T&FG will feed into the Information Governance Group to update and monitor progress and escalate any issues.	Task and finish group/ Head of Business Improvement and Modernisation/ Business and Risk Manager	31/10/2020
Risk Issue 2	**Training provision and record keeping of training is inconsistent and weak in some areas. There is a risk that staff are unaware of requirements to protect cardholders' data resulting in weak security of sensitive personal information.**		
Background Detail	There is a requirement with PCI DSS for all staff who take card payments, whether in person or over the phone, to receive training. This training should cover all aspects of card data security including, but not limited to: • recording of card numbers, • writing down numbers, • Repeating card numbers back to the customer. The training should be completed promptly when a new member of staff starts and a record kept of when it was completed.		
Action (Ref)	**Agreed Management Action**	**Responsibility**	**Deadline**
2.1	The Task and Finish Group to develop and agree training for all relevant staff.	Task and Finish Group	31/03/2020

Risk Issue 3	**Lack of policy or procedure to direct staff towards PCI DSS compliance.**		
Background Detail	Compliance with the PCI DSS is not a legal requirement though card providers (e.g. Visa, Mastercard) mandate compliance as part of their agreement. The current Information Security policy does have a section that covers the use of Chip and Pin and what our procedures should be in the event of a card data breach. However, it makes no mention of compliance with the standards or guidance as to what is required to achieve compliance.		
Action (Ref)	**Agreed Management Action**	**Responsibility**	**Deadline**
3.1	Set up a separate policy or procedures to cover the council's approach to compliance with the PCI-DSS to incorporate procedure to take in the event of a card data breach.	Task and Finish Group	31/03/2020

	This will link to other relevant policies such as the Information Security Policy and Data Protection Policy		

Risk Issue 4	**The council's various agreements with card providers may not offer value for money and make it difficult to administer as the card payment environment is more complex that it needs to be. Not only has this resulted in different fees and charges, there is an increased risk of vulnerabilities and non-compliance going undetected.**		
Background Detail	The council's main card provider 'Worldpay' charges are likely to rise over the coming years as more people opt to pay by card as the majority of these charges are made up of a 'per transaction fee' (the rate varies across the different agreements). When new payment systems are taken up, the software supplier invariably has their favoured card merchants which the council then signs up with rather than Worldpay. Other card merchant service providers should be explored to ensure that we are obtaining the best value for money, and ICT involved at an early stage to ensure compatibility. The possibility of obtaining a lower price across the board with one payment provider has been explored but have proved unsuccessful to date. Further small individual contracts would bring the total spent to a level requiring competitive tendering/exception report being completed to comply with contract procedure rules.		
Action (Ref)	**Agreed Management Action**	**Responsibility**	**Deadline**
4.1	Cost comparisons with card service providers to be explored. This will need to take into account the full costs, including per transaction costs. A report to be taken to SLT to give assurance that value for money is being achieved. Contracts/arrangements for card payments will be consolidated where possible.	Task and Finish Group	31/10/2020

Risk Issue 5	**PCI-DSS compliance is not always considered as part of procurement or contractual agreements with suppliers that take card payments on behalf of the council.**

Background Detail	The council does not request evidence that external service providers are compliant with PCI-DSS in order for them to receive money on its behalf. Some companies ask for the council to be compliant with PCI DSS as part of the contract; where the council is agreeing that it is compliant. One contract is nearing its end, with the option for monthly roll-on, has a requirement for cards to be preregistered with them before fees can be paid by card over the phone. The contract makes no reference to company being PCI DSS compliant, how long card data is retained for, or what they can use this data for. When the contract is finally terminated, clarification will be required as to how they will securely dispose of any card data relating to this contract.		
Action (Ref)	**Agreed Management Action**	**Responsibility**	**Deadline**
5.1	The Task and Finish Group will explore possible measures and update the procurement process (if deemed necessary) to ensure that PCI DSS is always considered when procuring card payment suppliers/services.	Task and Finish Group/procurement	31/03/2020
5.2	Include PCI-DSS as a requirements within Denbighshire Leisure's (ADM) contract T&Cs.	Legal Services Manager	31/03/2020

Appendix 1 – Risk Matrix and Assurance Ratings

Likelihood									
		>70%	Almost Certain	A					
	Event likely to occur in most circumstances	30–70%	Likely	B					
	Event will possibly occur at some time	10–30%	Possible	C					
	Event unlikely and may occur at some time	1–10%	Unlikely	D					
	Event rare and may occur only in exceptional circumstances	<1%	Rare	E					
					5	4	3	2	1
					Very Low	Low	Medium	High	Very High
			Service Performance		Minor errors or disruption	Some disruption to activities/ customers	Disruption to core activities/ customers	Significant disruption to core activities. Key targets missed	Unable to delivery core activities. Strategic aims compromised
			Reputation		Trust recoverable with little effort or cost	Trust recoverable at modest cost with resource allocation within budgets	Trust recovery demands cost authorisation beyond existing budgets	Trust recoverable at considerable cost and management attention	Trust severely damaged and full recovery questionable and costly
			Financial Cost (£)		<£50k	£50k – £250k	£250k – £1m	£1 m – £5 m	>£5m
					Impact				

Levels of Assurance		Definition	Management Intervention
	High Assurance	Risks and controls well managed and objectives being achieved.	Minimal action required, easily addressed by line management.
	Medium Assurance	Minor weaknesses in management of risks and/or controls but no risk to achievement of objectives.	Management action required and containable at service level. Senior management and SLT may need to be kept informed.

	Low Assurance	Significant weaknesses in management of risks and/or controls that put achievement of objectives at risk.	Management action required with intervention by SLT and / or CET.
	No Assurance	Fundamental weaknesses in management of risks and/or controls that will lead to failure to achieve objectives.	Significant action required in a number of areas. Require immediate attention from SLT or CET.

Report Recipients
• Chief Executive
• Head of Business Improvement and Modernisation
• Head of Legal, HR & Democratic Services
• Chief Accountant/ S151 Officer
• Chief Digital Officer
• Business and Risk Manager
• Business Continuity and ICT Security Officer
• Business Information Team Manager
• Legal and Procurement Operations Manager
• Team Leader – Communications & Campaign Management
• Strategic planning and Performance Officer
• Scrutiny Co-ordinator
• Corporate Director – Economic and Community Ambition
• Chair – Performance Scrutiny Committee
• Lead Member for Corporate Services and Strategic Direction
• Lead Member for Finance, Performance & Strategic Assets
• Corporate Governance Committee

Internal Audit Team		
Irene Griffiths	Auditor	01824706974 irene.griffiths@denbighshire.gov.uk

Key Dates	
Review commenced	July 2019
Review completed	August 2019
Reported to Corporate Governance Committee	20 November 2019
Proposed date for 1st follow up review	April 2020