PCI DSS compliance

Cabinet Member for Finance, Procurement, Customer Services and Revenues & Benefits

Date:	27 April 2021
Agenda Item:	4
Contact Officer:	Tracey Tudor
Tel Number:	01543 308225
Email:	tracey.tudor@lichfielddc.gov.uk
Key Decision?	**NO**
Local Ward Members	If any Wards are particularly affected insert the name of the Ward Members and their Ward. Ensure that the Ward Members have been consulted.

Lichfield district council

AUDIT & MEMBER STANDARDS COMMITTEE

1. Executive Summary

1.1 To provide an update to the Committee on the outstanding Payment Card Industry Data Security Standard (PCI-DSS) high priority recommendation.

2. Recommendations

2.1 To note the update.

3. Background

3.1 An audit assessment of e-payments was published in February 2017. The initial audit opinion was adequate assurance which means - 'there are some control weaknesses, but most key controls are in place and operating effectively. Some assurance can be given that the system, process or activity should achieve its objectives safely whilst achieving value for money. There is an average probability of loss (all asset types), fraud, impropriety, or damage to reputation'.

3.2 The audit concluded that were 7 actions (1 high, 5 medium and 1 low). To date 5 of the actions have been completed with 1 high and 1 medium action remaining outstanding. The Audit & Member Standards Committee have requested an update on the outstanding high recommendation which relates to the council's compliance with PCI-DSS.

3.3 The council complies with the PCI-DSS requirements for most payments. All payments made via direct debit, standing order, over the internet, the automated telephone line or at retail outlets, such as the Post Office or PayPoint points are fully compliant with the PCI-DSS requirements.

3.4 The only area that is not compliant is where staff are taking payments over the telephone and typing the card details into the payments system. The actual card information is not stored on any council IT system at any point as it is entered directly into a PCI-DSS compliant website provided by a third party. Once the payment has been submitted there is no way for council staff to retrieve the card information, even when making refunds as these are based on a separate unique code for the transaction issued by the authorising bank. There is also technology in Lichfield Connects that stops the card details from being recorded.

3.5 The technical controls outlined in paragraph 3.4 led to the approach of tolerating the non-compliance in favour of providing high quality customer services that supported those callers through the payment process. Additional managerial controls were in place in that the Lichfield Connects staff were working in the same office with managers and supervisors able to observe the actions of other staff throughout the working day. Further levels of assurance were gain by

subjecting the IT systems to annual health checks by ethical hackers to ensure they were secure as part of remaining on the central government secure network.

3.6 We want to encourage customers to continue paying on a regular basis, and there are a range of options available to resolve this issue and minimise the risk. In addition we want to embrace the opportunities that COVID-19 has presented following a change in our customer's behaviour along with taking into account the initial results of the live survey that we have underway whereby we are asking customer how they would prefer to interact with the Council. Early indications show that digital channels are our customers preferred way to interact with us. Therefore, in order to maximise these opportunities, we have made some initial changes to process –

- My team in Lichfield Connects will be promoting Direct Debits and alternative payment methods to those who are regular payers.
- As part of a trial - Lichfield Connects are no longer taking payments and are transferring customers to the payment line to ensure PCI compliance. We will gauge the feedback from customers following this change – if this is successful this will be rolled out to all colleagues.
- We have reviewed which of our processes require a payment to be made and identified some that are not digitally enabled - we will be sourcing solutions to ensure that they are digitally enabled.
- We are exploring new technology that will allow people to type in their own card details and maintain a high-quality contact experience.

3.7 There has also been the added complication of the contracts for the council's main finance system, this payments solution and the telephone platform. The contract for the finance system has been agreed and the new system is due to be implemented for October 2021. A proposal has been received for the payments solution and this is anticipated to lead to a new contract with three other Staffordshire council's commencing in September 2021. The future telephone platform is still being shaped and the ongoing survey on customer access channels will assist in setting the direction for the new ways of working. The replacement of the contact centre for one that supports PCI compliance was included in the Digital Strategy with the target delivery date of December 2021 following which we will re-apply to become recognised as being PCI-DSS compliant.

Alternative Options	1. None required.
Consultation	1. The Council's Section 151 Officer. 2. Customer Service Manager (interim)
Financial Implications	1. None noted.
Contribution to the Delivery of the Strategic Plan	1. Having sound arrangements for card payments contributes to the strategic plan objective of being 'a good Council'.
Equality, Diversity and Human Rights Implications	1. No equality, diversity or human rights implications arising from this report.

Crime & Safety Issues	1. None arising.

Environmental Impact	1. None arising.

GDPR/Privacy Impact Assessment	1. This update is to provide assurance to the Committee of the progress made on improving the Council's internal control environment in respect of electronic payments.

	Risk Description	How We Manage It	Severity of Risk (RYG)
A	Continuing non-compliance with the PCI-DSS results in reputational or financial impacts.	The managerial and technical controls described in the paper led to the risk being tolerated. This is being addressed through new financial, payment and telephony contracts which fully support the PCI-DSS standard.	Likelihood - Green Impact – Yellow Severity of Risk – Yellow (tolerable)

Background documents

Internal Audit Progress Reports
Minutes of the Audit & Member Standards Committee

Relevant web links