North Lanarkshire Council
Report

Audit and Scrutiny Panel

☐ approval ☒ noting **Ref** KH/RL/GL **Date** 10/12/20

Update on status/actions to secure PCI-DSS compliance

From Katrina Hassell, Head of Business Solutions

Email HassellK@northlan.gov.uk **Telephone** 01698 302235

Executive Summary

The purpose of this report is to provide the Panel with an overview of the Council's project plan for achieving compliance with the Payment Card Industry Data Security Standard (PCI DSS).

This report summarises the main steps that are in progress and planned to happen for PCI DSS compliance to be achieved. It also states identified risks that may affect project completion.

Recommendations

The Panel is invited to:

(1) Note the content of the report, and actions associated with delivering compliance, and;
(2) Note that significant work is still required to achieve compliance within the timeframe set.

The Plan for North Lanarkshire

Priority All priorities

Ambition statement All ambition statements

1. Background

1.1 Elected members will recall that the council permits payment for a wide range of services to be made using credit and debit cards.

1.2 In 2006 those companies which provide payment card banking services formed the PCI Security Standards Council (SSC). The SSC in turn created a set of security standards for safe payments worldwide, known as the PCI Data Security Standard. Acquiring banks have informed organisations that they must comply with PCI DSS requirements in order to continue accepting card payments.

1.3 As of the October 2019 PCI DSS assessment, a lack of formal ownership within Council services saw the Council fall into a state of non-compliance. The issue was highlighted during a change of Merchant Acquiring Bank, with Lloyds Cardnet highlighting non-compliance could lead to potential contract termination. Given this would result in the Council being unable to process card transactions, steps were taken to address this immediately.

1.4 Remedial action was undertaken jointly by Financial Services and Business Solutions, which with the aid of Lloyds Cardnet PCI DSS Compliance team, resulted in enough compliance being achieved to enable card transactions to continue. However, this solution is short-term, and further actions and governance must be implemented to maintain compliance longer-term.

1.5 Through discussion at the Audit and Scrutiny Panel meeting of 3 September 2020, Business Solutions has set a target date for achieving compliance with PCI DSS requirements of September 2021. To this end a project plan has been developed that identifies the main steps that require to be performed to meet that timeframe.

---

2. Planning for PCI DSS Compliance

Identification of Headline Activities

2.1 The council's proposed PCI DSS roadmap covers six main stages:

a) Discovery & Scoping
b) Evaluation & Scope Minimisation
c) Gap Analysis
d) Options Appraisal & Selection
e) Implementation of Remedial Actions
f) Maintain and Monitor

2.2 Whilst the headline steps outlined above provide an overarching breakdown to the methodology behind project managing this compliance exercise, a more comprehensive project plan has been developed. This is shown in Appendix A of this report.

Discovery & Scoping

2.3 Discovery is where the flows of relevant cardholder data (card number, name of cardholder, expiry date, and card verification value) are identified. Once touch points and network cardholder data flows are identified, the cardholder data environment can be scoped. The main aim of the discovery phase is to:

- Identify how and where the organization receives cardholder data;
- Locate and document where cardholder account data is stored, processed, and transmitted;
- Identify all other system components, processes, and personnel that are in scope;
- Implement controls to minimize scope to necessary components, processes, and personnel.

2.4 It should be noted that scoping involves more than simply identifying network or ICT touch points for cardholder data. It encompasses gaining a thorough understanding of the people, processes and technologies involved in storing, processing and/or transmitting of cardholder data. In effect, the cardholder data environment isn't something that exists only in terms of technology: people and process are also part of that environment.

Evaluation and Scope Minimisation

2.5 Evaluation and scope minimisation can be thought of as an extension of discovery and scoping. However, by this stage the project is moving from effectively being a data collection exercise to analysis and design. This is because a major theme within any initial PCI DSS assessment is segmentation, or scope minimisation. This means limiting connectivity between the cardholder data environment and other systems to only that which is necessary. Systems which exist outside of the cardholder data environment, but which interact with systems processing cardholder data, are themselves subject to PCI DSS conditions.

2.6 The interconnected nature of North Lanarkshire Council (NLC) systems, combined with overlapping staff roles with no clear segregation from PCI DSS tasks, results in a challenging environment for PCI DSS compliance. To restrict the scope of compliance, it will be necessary to ensure those systems that process cardholder data are effectively segmented from the wider council network. As well as technology, the cardholder data environment should be segmented from people and processes that do not need to interact with or influence the cardholder data environment.

Gap Analysis

2.7 Having defined the cardholder data environment, and the applicable PCI DSS requirements needing to be put in place, it will be necessary to understand where gaps in requirements exist and options for addressing these. Some may be relatively straightforward, such as developing a security policy that reflects PCI DSS requirements, others more complex.

2.8 Not all requirements can be addressed by technology, many relate to people and processes. Given the numerous payment systems and channels which exist across both Culture and Leisure North Lanarkshire (CLNL) and NLC, significant gaps will be identified along with a need to adopt new business processes for taking cardholder payments in a PCI DSS compliant manner.

Options Appraisal and Selection

2.9 In considering gaps against PCI DSS requirements there may be alternative solutions each with associated varying costs and benefits. These will be assessed through an options analysis to determine that which best fits the council's environment.

Implementation of Remedial Actions

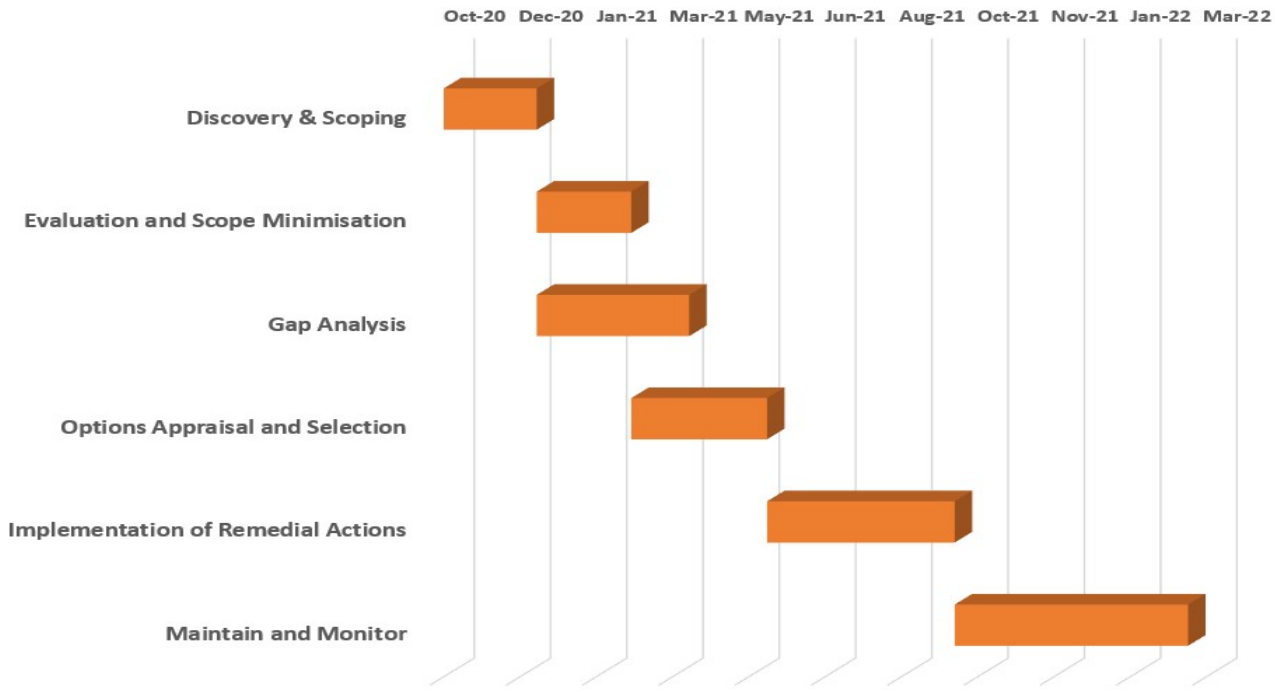
2.10 This is the stage where all applicable PCI DSS requirements not yet in place will be implemented.

2.11 NLC is a Level 4 merchant based on the number of annual card transactions, taken through all mechanisms of Electronic Point of Sale (Epos) and Card Holder not Present (CNP). This places the council into a complex self-assessment bracket that comprises approximately 300 applicable condition statements. Although dependent upon findings from the gap analysis, that suggests an intensive exercise may need to be invoked to ensure these remedial actions be implemented within the timeframe that NLC has committed to. However, until the gap analysis is complete that remains a known unknown.

Maintain and Monitor

2.12 Once compliance has been achieved it will require to be maintained. A suite of processes and checks will require to be put in place to ensure compliance is maintained and becomes a factor to be considered during changes to any part of the cardholder data environment.

2.13 The overall timeline for delivering all steps identified above is as follows:



Project Risks

2.14 Monitoring of project risk will be critical in assuring the project plan stays on schedule. Risks have been identified and will be monitored as the project progresses. These are listed in Appendix B.

Next Steps

2.15 Following review of the range of information presented to the Panel, Members are asked to continue to be aware of the complexity of obtaining PCI DSS compliance and to note that continued compliance can only be obtained through good governance, informed risk management and appropriate service engagement to ensure progress.

3. Equality and Diversity

3.1 **Fairer Scotland Duty**
There is no requirement to carry out a Fairer Scotland Duty assessment on this report.

3.2 **Equality Impact Assessment**
There is no requirement to carry out an equality impact assessment on this report.

4. Implications

4.1 **Financial Impact**
There is no immediate financial impact arising from this report, but possible future costs associated with this compliance programme should be noted.

4.2 **HR/Policy/Legislative Impact**
The council will be able to demonstrate effective security around the taking of card payments and meet requirements levied by the PCI SSC and through the Data Protection Act 2018.

4.3 **Environmental Impact**
There is no environmental impact arising from this report.

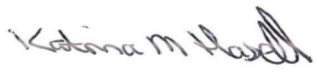
4.4 **Risk Impact**
Risks are documented within Appendix B of this report.

5. Measures of success

5.1 The council continues to efficiently and effectively handle card payments to provide benefit to users of North Lanarkshire Council services.

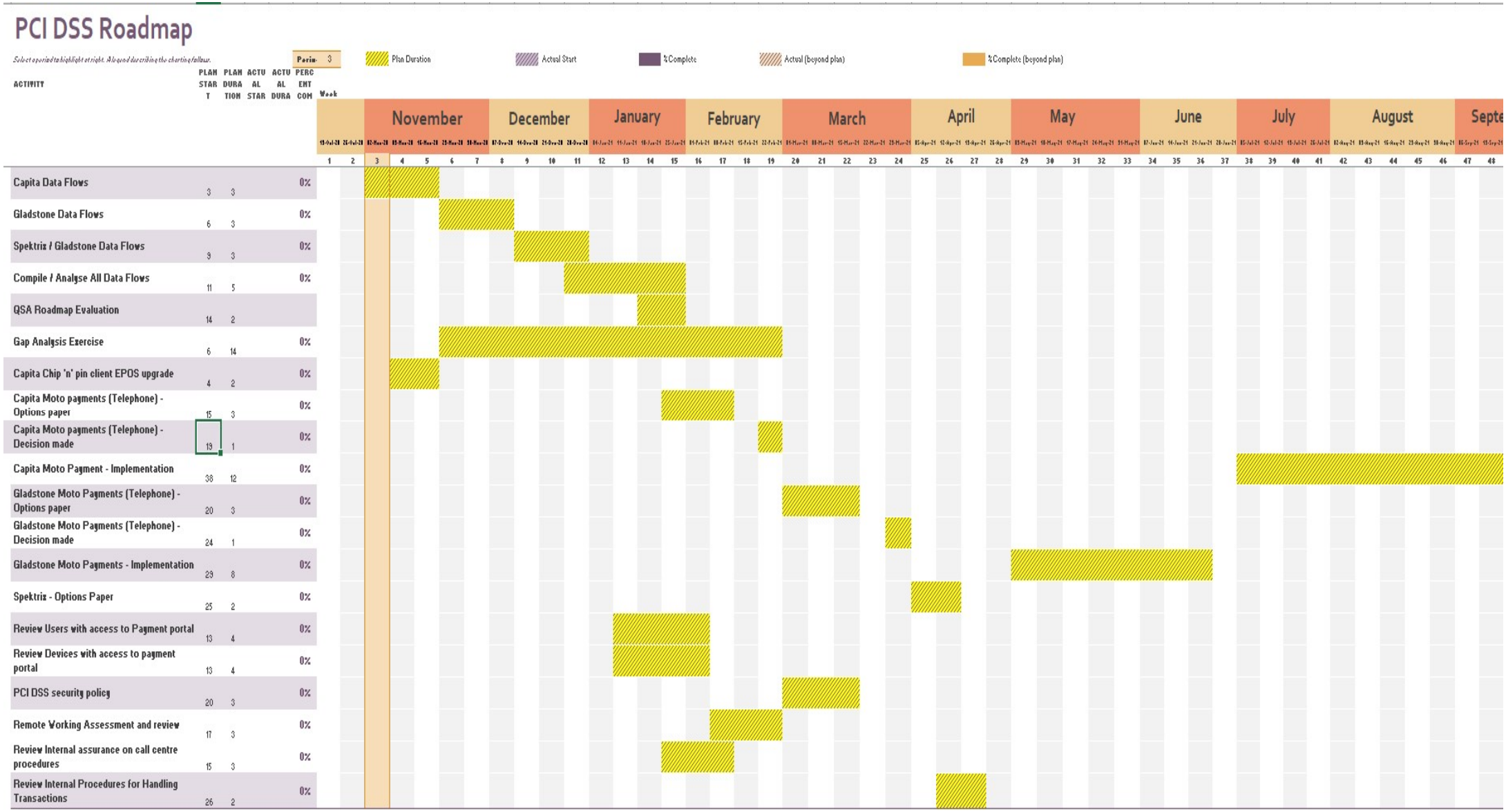
6. Supporting documents

6.1 None



Head of Business Solutions

Appendix A: PCI DSS Roadmap as at 10/11/2020



Appendix B: Project Risks

The following table highlights risks that may affect completion of this project within the target timeframe:

Ref.	Risk	Comments/Control
R001	System changes may occur as the project is under way which may alter the scope of the initial cardholder data environment.	It is proposed that such changes be captured by ensuring a PCI DSS lead represent the different parts of NLC where card payments are taken. Currently representation has been obtained from what historically was each of Culture North Lanarkshire, North Lanarkshire Leisure, and North Lanarkshire Council.
R002	Lack of PCI DSS knowledge and experience, which in turn may lead to incorrect assumptions at the planning stage, mean the project skews significantly off a true and proper course.	It is proposed to bring a Qualified Security Assessor on board to perform an initial review of the cardholder data environment and confirm the proposed project plan and timelines are accurate and pragmatic.
R003	Lack of project management capability results in the project becoming badly coordinated and progress delayed.	It is proposed to ensure a dedicated individual act as project manager and invoke regular project review through putting a governance board in place. The person appointed as project manager will be skilled in this area or have enough support to ensure the project operates in a well-defined manner.
R004	There is a risk that the financial cost of becoming PCI DSS compliant is perceived to outweigh any appetite to do so.	Cost will be captured through effective business impact and cost benefit analysis. Ownership of PCI DSS compliance will be clearly stated and the risks of not being compliant assigned a fit and appropriate owner. A project owner will be identified to ensure the cost of transitioning to a PCI DSS compliant state is monitored and communicated to the risk owner for compliance.
R005	A lack of resource results in insufficient capability for the project to succeed.	A suitably senior individual will be appointed as project sponsor who will have the authority and influence to ensure resource will be made available, from across the council and other stakeholder organisations, as required.
R006	The insourcing of CLNL may result in changes to the cardholder data environment after discovery has been completed, resulting in incorrect information being used to deliver compliance.	It is proposed that such changes be monitored through ensuring links are in place between those responsible for managing the insourcing and PCI DSS stakeholders.
R007	Staffing resources may become stretched at certain times of the year, or ICT system change freezes occur, putting pressure on the ability to stay to the proposed timeframe, in turn resulting in project delays.	End of financial year processes and the extension of the leave year to end March 2021 are examples of why such pressures may arise. It is proposed to manage this risk through ensuring stakeholders in the PCI DSS project are made aware of proposed timeframes, and that these are agreed with business owners in advance.