Report to	Corporate Governance Committee
Date of meeting	22 January 2020
Lead Member / Officer	Lisa Lovegrove – Chief Internal Auditor
Report author	Lisa Lovegrove – Chief Internal Auditor
Title	Internal Audit of Payment Card Industry Data Security Standards (PCI-DSS)

1. What is the report about?

This report provides details of a recent Internal Audit report of Payment Card Industry Data Security Standards (PCI-DSS) that received a 'Low' assurance rating.

2. What is the reason for making this report?

Corporate Governance Committee has agreed that it will receive and discuss all Internal Audit report receiving a 'Low' assurance rating so that they can discuss the outcome and receive assurance that improvements will be made.

3. What are the Recommendations?

That the Committee comments on the report and decides whether it requires any further update reports on progress with the improvement action plan.

4. Report details

We carried out this review of PCI-DSS to check compliance with the information security standard for handling credit or debit card payments. While compliance is not a legal requirement, card merchants and software suppliers often ask for compliance as part of their contractual agreements.

The review focused on: roles and responsibilities, policy and procedures, training, payment card environment, processing card payment data, third party processor compliance and compliance testing and self-assessment.

Our review highlighted issues relating to the lack of a programme or strategy to ensure compliance with the PCI-DSS. Training is inconsistent across services and awareness of proper practices is weak in some areas due in part to the absence of corporate policy or procedures to direct consistency.

The council has various agreements with card providers making the card payment environment more complex than it needs to be and therefore difficult to manage and demonstrate value for money. Also, PCI-DSS compliance was not considered as part of some historic procurement and contractual agreements with suppliers that take card payments on behalf of the council. As a results, some contracts do not state that compliance with the standards is required. We are aware that this is now included as part of the procurement process.

While there are areas of good practice and no instances of security breaches involving card payments had been identified; we give a low assurance rating due to the nature of the issues and controls weaknesses. Cooperation across all services is required to drive the necessary improvement and so the results of this review has been reported to the Information Governance Group and to the Senior Leadership Team to obtain their backing.

Further information is available in the Internal Audit report – see Appendix 1.

5. How does the decision contribute to the Corporate Priorities?

Not applicable – there is no decision required with this report.

6. What will it cost and how will it affect other services?

Not applicable – there is no decision required with this report.

7. What are the main conclusions of the Well-being Impact Assessment?

Not applicable – there is no decision required with this report.

8. What consultations have been carried out with Scrutiny and others?

Not applicable – there is no decision required with this report.

9. Chief Finance Officer Statement

Not applicable – there is no decision required with this report.

10. What risks are there and is there anything we can do to reduce them?

Not applicable – there is no decision required with this report.

11. Power to make the decision

Not applicable – there is no decision required with this report.