



**Report Reference Number: A/18/4**

---

**To: Audit and Governance Committee**  
**Date: 25 July 2018**  
**Authors: Phil Jeffrey; Audit Manager – Veritau**  
**Lead Officer: Karen Iveson; Chief Finance Officer**

---

**Title: Consideration of Internal Audit reports**

**Summary:**

The Chair of the Audit & Governance Committee receives internal audit reports where the opinion of the auditor is 'Limited Assurance' or 'No Assurance'.

The internal auditor, Veritau has completed an audit of the Payment Card Industry Data Security Standard (PCI DSS) at the Council. The report concludes that the overall opinion of the audit was that the controls within the system provide 'Limited Assurance'. The report is provided (Appendix A) for the Audit & Governance Committee to consider.

**Recommendation:**

**To consider the Internal Audit report which relates to PCI DSS.**

**Reasons for recommendation**

To enable the committee to fulfil its responsibility for reviewing the outcomes of internal audit work.

**1. Introduction and background**

- 1.1 Veritau completed an audit of PCI DSS and the final report was issued on 12<sup>th</sup> July 2018.
- 1.2 Internal audit reports completed by Veritau give an overall audit opinion based on five grades: High Assurance, Substantial Assurance, Reasonable Assurance, Limited Assurance and No Assurance.

1.3 Audits where an opinion is provided of Limited or No Assurance are brought to this committee for presentation and discussion.

## **2. The Report**

2.1 The report sets out the findings of the internal audit of PCI DSS.

2.2 The purpose of the audit was to provide assurance to management that effective controls have been put in place to manage compliance with the PCI DSS. It covered the following key elements of compliance, to establish whether the Council has:

- documented all systems and processes subject to the PCI DSS;
- compliance assurance processes in place from third-party payment processors acting on its behalf;
- up to date guidance in place for all Council staff who process card payments;
- submitted annual self-assessment questionnaires and attestations of compliance with PCI DSS.

2.3 The report concluded that the arrangements for managing risk were poor with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided Limited Assurance.

2.4 The report forms the basis for discussion at the Audit & Governance Committee meeting. The Committee will have the opportunity to ask questions of officers and the internal auditors at the meeting. The Committee can then make recommendations to the Executive or Council as appropriate.

## **3. Legal/Financial Controls and other Policy matters**

3.1. Legal Issues

(a.) None.

3.2. Financial Issues

(a.) None.

## **4. Conclusion**

4.1 The Committee is asked to consider the report.

## **5. Background Documents**

None.

**Contact Officer:** *Phil Jeffrey; Audit Manager - Veritau*  
[phil.jeffrey@veritau.co.uk](mailto:phil.jeffrey@veritau.co.uk)  
*01904 552926 / 01757 292281*

**Appendices:** **Appendix A: PCI DSS internal audit report 2017/18.**