East Lothian Council

REPORT TO: Audit and Governance Committee

MEETING DATE: 18 September 2012

BY: Executive Director (Support Services)

SUBJECT: Internal Audit Report – Payment Card Industry Data Security Standard

---

1 PURPOSE

1.1 To inform the Audit and Governance Committee of the recently issued audit report on the Payment Card Industry Data Security Standard (PCI DSS).

2 RECOMMENDATIONS

2.1 That the Audit and Governance Committee note the contents of the Executive Summary and Action Plan for the PCI DSS.

3 BACKGROUND

3.1 A review of the PCI DSS was undertaken as part of the audit plan for 2012/13.

3.2 The main objective of our review was to ensure that the Council has appropriate arrangements in place for compliance with the PCI DSS.

3.3 The main findings from our audit work are outlined in the attached report.

4 POLICY IMPLICATIONS

4.1 None

5 EQUALITIES IMPACT ASSESSMENT

5.1 This report is not applicable to the well being of equalities groups and Equality Impact Assessment is not required.

6 RESOURCE IMPLICATIONS

6.1 Financial - None

6.2 Personnel - None

6.3 Other - None

7 BACKGROUND PAPERS

7.1 None

AUTHOR'S NAME	Mala Garden
DESIGNATION	Internal Audit Manager
CONTACT INFO	01620 827326
DATE	7 September 2012

EAST LOTHIAN COUNCIL – INTERNAL AUDIT
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

1. EXECUTIVE SUMMARY

1.1 Introduction

As part of the Audit Plan for 2012/13, Internal Audit reviewed the arrangements in place across the Council to ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS).

1.2 Areas where Expected Controls were Met

- The payment processing function for card payments is undertaken by suppliers who are PCI DSS compliant, reducing the risks to the Council associated with certain PCI DSS requirements.

1.3 Areas with Scope for Improvement

- There was a lack of clear ownership and responsibility for ensuring that the Council meets the requirements of the PCI DSS. *Risk – non-compliance leading to fines, penalties, increased transactional costs and an inability to process card payments.*
- At present the complete card payment environment, including all processes that involve PCI related data, has not been clearly identified and documented. *Risk – failure to identify all key aspects of the storage, processing and transmitting of payment card data.*
- A consistent approach was not adopted across the Council for the processing of cardholder data – different systems and suppliers are currently used throughout the Council for accepting card payments. *Risk – increased vulnerability of the card payment environment.*
- The storage, retention and destruction of cardholder data require review. *Risk – non-compliance with PCI DSS requirements.*
- No arrangements are currently in place to validate compliance with PCI DSS requirements – an annual self assessment questionnaire has not been completed and quarterly scans have not been programmed. *Risk – failure to identify control deficiencies.*
- There was a lack of procedures and training in place for staff dealing with card payments. *Risk – breaches in data security may occur.*

1.4 Summary

Our review of the Payment Card Industry Data Security Standard identified a number of areas with scope for improvement. Detailed recommendations and opportunities for improvement are contained in our main Audit Report.

Mala Garden
Internal Audit Manager **September 2012**

ACTION PLAN

PARA REF	RECOMMENDATION	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.1.1	Ownership and responsibility for ensuring that the Council meets the compliance requirements of the Payment Card Industry Data Security Standard should be clearly identified – a Senior Officer should be assigned responsibility for this area.	Executive Director (Support Services)	Agreed – A senior officer will be assigned responsibility for this area.		September 2012
3.2.1	Detailed corporate procedures should be drawn up to ensure that all staff dealing with card payments comply with the Payment Card Industry Data Security Standard.	Executive Director (Support Services)	Agreed		March 2013
3.2.2	Management should ensure that the Council's complete card payment environment is clearly identified and documented. Management should review the existing arrangements whereby different systems are used for payment processing – consideration should be given to rationalising the card payment process.	Executive Director (Support Services)	Agreed		December 2012

PARA REF	RECOMMENDATION	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.3.1	**Management should ensure that arrangements are in place to validate compliance with the Payment Card Industry Data Security Standard – the annual Self Assessment Questionnaire should be completed.** **Management should consider whether expertise currently exists within the Council to carry out the required self assessment or whether an external qualified assessor should be appointed.** **A timetable for the completion of the annual Self Assessment Questionnaire should be established and quarterly network scans programmed.**	**Executive Director (Support Services)**	**Agreed**		**December 2012**
3.4.1	**Management should ensure that the draft Corporate Retention Schedule is finalised.** **For cardholder data, the Corporate Retention Schedule should strictly limit storage and retention time to that which is required for business, legal and/or regulatory purposes.** **A consistent approach should be adopted in respect of the storage, retention and destruction of cardholder data, which is fully compliant with PCI DSS requirements.**	**Records Manager**	**Agreed**		**January 2013**

PARA REF	RECOMMENDATION	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.5.1	**Management should review the existing list of Paye.net users, with a view to restricting access to users who are required to accept card payments as part of their duties.** **Appropriate arrangements should be put in place to notify the Revenues Systems and Control Team of all leavers to enable access rights to be removed timeously.** **Management should consider whether it is appropriate for employees to have access to Paye.net while they are working from home.**	**Executive Director (Support Services)**	**Agreed**		**March 2013**
3.6.1	**Appropriate training on PCI DSS requirements should be provided to all staff members dealing with card payments.**	**Executive Director (Support Services)**	**Agreed**		**March 2013**