BRIDGEND COUNTY BOROUGH COUNCIL

REPORT TO AUDIT COMMITTEE

8 NOVEMBER 2007

REPORT OF THE CHIEF INTERNAL AUDITOR

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

1. Purpose of Report.

1.1. To update members on progress on the Council's response to the Payment Card Industry Data Security Standards (PCI/DSS).

2. Connection to Corporate Improvement Plan / Other Corporate Priority.

2.1. Internal Audit's work impacts on all of the Corporate Improvement Plan/other corporate priorities.

3. Background.

3.1. PCI DSS is a worldwide standard that has been in existence for some time but has recently been amended and is being more strongly enforced by the payment card industry. From 30 June 2007, all organisations that process, store or transmit credit or debit card details have had to conform to this requirement. The standards apply regardless of the payment method; telephone, online, mail and over-the-counter services. Those who fail to comply fully with the PCI DSS can be liable for punitively large fines or even barred from card acceptance schemes completely.

3.2. To comply, organisations will need to perform mandatory quarterly and/or annual security audits. Violating just one of the requirements without compensating controls triggers overall non-compliance.

4. Current situation

4.1. Compliance with these standards are proving a challenge to organisations throughout the world and BCBC is no exception. However their importance is recognised by management and Internal Audit is working closely with IT, through the IT Security Forum, to deliver compliance.

4.2. There are different levels of compliance depending upon the number of card transactions the organisation takes. BCBC falls into the category of compliance which requires the completion of an annual Self Assessment Questionnaire (SAQ) and network vulnerability scans conducted by an Approved Scanning Vendor (ASV).

4.3. The supplier of our cash system has developed enhanced security software but as this has not be formally signed off yet, BCBC has had a formal extension from our bank until 31st December.

4.4. As the SAQ is primarily technical, the I.T. Department is responsible for completing it. The questionnaire will be forwarded to the bank with a statement specifying any risk mitigation measures that have been put in place.

4.5. BCBC already undergo a quarterly Penetration test conducted on its network by NCC, who is an ASV, and the scans required by the PCI/DSS has been combined with this.

4.6. The latest test on the 11th October flagged up some areas that required attention. This was discussed at the IT Security Forum and measures are being put in place to rectify the situation. As part of the process, internal penetration testing will be carried out as well as a re-test by our external supplier.

4.7. Although all this is achievable by the 31st December, Members should be aware that it is a tight timeframe.

5. Effect upon Policy Framework& Procedure Rules.

5.1. None

6. Legal Implications.

6.1. None

7. Financial Implications.

7.1. None

8. Recommendation.

8.1. That Members note the report

Nyall Meredith

Chief Internal Auditor

31 October 2007

Contact Officer: Nyall Meredith

Chief Internal Auditor

Telephone: (01656) 754901

E-mail: nyall.meredith@bridgend.gov.uk

Postal Address

Bridgend County Borough Council
Brackla House
Brackla Street
Bridgend
CF31 1BZ

Background documents

None