



Dacorum Borough Council

Final Internal Audit Report

Payment Card Industry Data Security Standard (PCI DSS)

December 2015

This report has been prepared on the basis of the limitations set out on page 11.

CONFIDENTIAL

Distribution List:

John Worts – Information Security Manager

Mark Brookes – Group Manager (Legal Governance and Deputy MO)

Steve Baker – Assistant Director (Chief Executive's Unit/MO)

David Skinner – Assistant Director (Finance and Resources)

James Deane – Corporate Director (Finance and Operations) (Final Report only)

Sally Marshall – Chief Executive (Final Report only)

Key Dates:

Date of fieldwork: August 2015

Date of draft report: November 2015

Receipt of responses: December 2015

Date of final report: December 2015

This report and the work connected therewith are subject to the Terms and Conditions of the Contract dated 1 April 2015 between Dacorum Borough Council and Mazars Public Sector Internal Audit Limited. This report is confidential and has been prepared for the sole use of Dacorum Borough Council. This report must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law, we accept no responsibility or liability to any third party who purports to use or rely, for any reason whatsoever, on this report, its contents or conclusions.

Contents

1. Executive Summary 1

2. Scope of Assignment 3

3. Assessment of Control Environment..... 4

4. Observations and Recommendations 5

Recommendation 1: Inadequate Secure Socket Layer Security (Priority 2)..... 5

Recommendation 2: Vulnerability patch management (Priority 2) 6

Recommendation 3: Point of Sale / Point of Interaction device compliance (Priority 2). 7

Recommendation 4: Capita Services PCI DSS compliance verification status (Priority 3). 8

Appendix A - Reporting Definitions 9

Appendix B - Staff Interviewed..... 10

Statement of Responsibility..... 11

1. Executive Summary

1.1. Background

We have completed a compliance audit assessment of the Council's systems of internal control in respect of the Payment Card Industry Data Security Standard (PCI DSS) ver 3.1 April 2015 to assess the extent to which the reputational damage and financial risks are mitigated. The total value of 2014/2015 debit and credit cards transactions is £135k which reduces to £34k if the Capita processed Touchtone Telephone and Internet Payment receipts are excluded.

Many organisations who had already committed resources on complying with the 2014 PCI DSS Version 3.0, which took effect on 31st December 2014, were taken by surprise when the Payment Card Industry Security Standards Council released a new version of the PCI DSS Standard in April 2015, ahead of the usual 3 year release cycle which had immediate effect.

1.2. Audit Objective and Scope

The overall objective of this audit was to provide assurance over the adequacy and effectiveness of current control environment in respect of the Payment Card Industry Data Security Standard (PCI DSS) ver 3.1 April 2015 and provide recommendation guidance on how to improve the current controls going forward.

In summary, the audit scope covered the following areas:

- Build and Maintain Secure Network Policies;
- Protect Cardholder Data;
- Vulnerability Management Program;
- Implement Strong Access Controls;
- Regularly Monitor and Test Networks;
- Maintain an Information Security Policy.

Further detail on the scope of the audit is provided in Section 2 of the report.

1.3. Summary Assessment

Our audit of DBC's internal controls operating in respect of the 2015 Payment Card Industry Data Security Standard (PCI DSS) ver 3.1 found that there is a sound system of internal control designed to achieve the system objectives. Also, there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Our assessment in terms of the design of, and compliance with, the system of internal control covered is set out below:

Evaluation Assessment	Testing Assessment
Full	Substantial

Management should be aware that our internal audit work was performed according to UK Public Sector Internal Audit Standards (PSIAS) which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board. Similarly, the assurance gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Similarly, the assessment gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board. The classifications of our audit assessments and priority ratings definitions for our recommendations are set out in more detail in Appendix A, whilst further analysis of the PCI-DSS control environment is shown in Section 3.

1.4. Key Findings

We have raised three priority 2 and a single priority 3 recommendation where we believe there is scope for improvement within the PCI-DSS control environment. These are set out below:

- Secure Socket Layer - All and any existing use of SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. (Priority 2)
- Vulnerability patch management – Appropriate key performance indicators and vulnerability compliance monitoring reports should be established and applied.(Priority 2)
- Compliance verification checks on all Point of Sale device assets.(Priority 2)

- CAPITA Services PCI DSS compliance verification status documentation. (Priority3)

Full details of the audit findings and recommendations are shown in Section 4 of the report.

1.5. Management Response

We received the management responses in a timely manner and these have been included in the main body of the report.

1.6. Acknowledgement

We would like to take this opportunity to thank all staff involved for their time and co-operation during the course of this visit.

2. Scope of Assignment

2.1. Objective

The overall objective of this compliance audit was to provide assurance that the systems of control in respect of the 2015 Payment Credit Industry Data Security Standard (PCI-DSS version 3.1) is effective and consistently applied.

2.2. Approach and Methodology

The audit approach was developed by an assessment of risks and management controls operating within each area of the scope and the following procedures were adopted to enable us to recommend control improvements:

- Hold discussions with key members of staff to ascertain the operational controls;
- Identification of the role and objective of each area of scope;
- Identification of risks relating to the auditable area and the controls in place that enable the control objectives to be achieved;
- Evaluation and testing of controls within the system;
- Discussion of our findings with management and further development of our recommendations; and
- Preparation and agreement of a draft report with the process owner.

2.3. Areas Covered













The audit was carried out to evaluate and test controls over the following areas:

- **Build and Maintain a Secure Network Policies:**
 1. Install and maintain a firewall configuration to protect cardholder data;
 2. Do not use vendor-supplied defaults for system passwords and other security parameters;
- **Protect Cardholder Data:**
 3. Protect stored cardholder data;
 4. Encrypt transmission of cardholder data across open, public networks;
- **Maintain a Vulnerability Management Program:**
 5. Use and regularly update anti-virus software on all systems commonly affected by malware;
 6. Develop and maintain secure systems and applications;
- **Implement Strong Access Control Measures:**
 7. Restrict access to cardholder data by business need-to-know;
 8. Assign a unique ID to each person with computer access;
 9. Restrict physical access to cardholder data;
- **Regularly Monitor and Test Networks:**
 10. Track and monitor all access to network resources and cardholder data;
 11. Regularly test security systems and processes;
- **Maintain an Information Security Policy:**
 12. Maintain a policy that addresses information security.

3. Assessment of Control Environment

The following table sets out in summary the control objectives we have covered as part of this audit, our assessment of risk based on the adequacy of controls in place, the effectiveness of the controls tested and any resultant recommendations.

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

Control Objectives Assessed	Design of Controls	Operation of Controls	Recommendations Raised
Build and Maintain Secure Network Policies			
Protect Cardholder Data			Recommendation 1
Vulnerability Management			Recommendation 2
Access Controls			Recommendation 3
Monitor and Test Networks			Recommendation 4
Maintain an Information Security Policy			

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

4. Observations and Recommendations

Recommendation 1: Inadequate Secure Socket Layer Security (Priority 2)

<p>Recommendation</p> <p>In compliance with PCI-DSS (version 3.1 requirement 4.1), the Council must ensure that:</p> <ul style="list-style-type: none"> a) SSL and early TLS are no longer used as a security control after June 30, 2016. b) Effective immediately, new implementations MUST NOT use SSL or early TLS. c) All and any existing use of SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
<p>Observation</p> <p>The 2015 payment card industry data security standard PCI-DSS (version 3.1 requirements 4.1) mandates that specific security controls are established and applied to mitigate the known risks of the Secure Socket Layer (SSL) computer protocol.</p> <p>Examination of the recent external IT Security Test report noted that SSL V3 was identified in use at the Council. This resulted in a medium risk issue for the Council to address. [Page 11 - "Description of the Issue - An attacker could affect the confidentiality of data that has been transmitted using SSLv3.0 by exploiting a flaw in the way the protocol handles padding of bytes. This issue has been publically announced as POODLE (Padding Oracle On Downgraded Legacy Encryption) and SSL version 3 should therefore not be relied upon].</p> <p>There is an increased risk of non compliance with the 2015 PCI-DSS (version 3.1 requirement 4.1) until the Council can ensure that:</p> <ul style="list-style-type: none"> a) SSL and early TLS are no longer used as a security control after June 30, 2016. b) Effective immediately, new implementations MUST NOT use SSL or early TLS. c) All and any existing use of SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
<p>Responsibility</p> <p>Information Security Manager / ICT</p>
<p>Management response / deadline</p> <ul style="list-style-type: none"> a) A review will need to be performed on servers Capita Live and Capita Test to establish if they are using SSL / early TLS – review to be completed by 31st December 2015 b) Request from Capita that new implementations will not be using SSL or early TLS. DBC ICT must also configure new implementations using either TLS IPSEC or SSH. This will be a server configuration document from Capita – expected by 31st January 2016 c) Linked to a) – If applicable (i.e. if we are still using SSL or early TLS) a Migration Plan and Risk Mitigation to be in place by 28th February 2016

Recommendation 2: Vulnerability patch management (Priority 2)

<p>Recommendation</p> <p>Key performance indicators should be established and applied to demonstrate the extent to which vulnerability patch management issues and penetration test report concerns, such as weak passwords, are effectively monitored for resolution.</p>
<p>Observation</p> <p>The 2015 payment card industry data security standard PCI-DSS (version 3.1 requirements 6.1) mandates that policies and procedures are defined and applied to identify new security vulnerabilities and also mandates (6.2) that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied critical security patches within one month of release.</p> <p>Dacorum’s IT Security Policy states that “The Council acts to identify and patch software and system vulnerabilities” and Microsoft System Centre Configuration Manager Tool was confirmed in use to help ensure that all hosts are patched against known vulnerabilities. However, examination of the key documents confirmed that while the Council uses reputable outside sources to provide information on IT security, the recent internal security test report identified that weak passwords were identified and patch management activities were ineffective on 28 hosts within the network. The existence of one critical vulnerability had allowed the security test team to exploit a vulnerability and gain full admin rights to the IT network.</p> <p>There is an increased risk that the Council may fail to comply with the PCI-DSS requirement to apply all vendor-supplied critical security patches within one month of release unless vulnerability management reports and key performance indicators are established and applied to demonstrate the PCI-DSS compliance requirements are effectively monitored for achievement.</p>
<p>Responsibility</p> <p>Information Security Manager</p>
<p>Management response / deadline</p> <p>We have a patch management policy;</p> <ul style="list-style-type: none"> • Servers – split into four farms done every Monday between the hours of 00.00 and 02.59 AM Patches for Windows Security and Critical Updates are applied. • Hosts – Patched Daily with Microsoft Security and Critical Updates • 3rd Party Applications (Adobe and Java etc.) – Patched with critical updates monthly. • Vendor Patches are applied via RFC and subject to approval by Change Control Board. • Microsoft SCCM 2012 is the mechanism used to measure and monitor patches on all systems in the domain. <p>All remedial actions in the internal remedial action plan (R.A.P) have now been applied and approved by Cabinet Office on 2nd November 2015 as part of the Public Sector Network (PSN) approval process.</p>

Recommendation 3: Point of Sale / Point of Interaction device compliance (Priority 2)**Recommendation**

Management should ensure that:

- a) All passwords and default accounts are confirmed as compliant; and
- b) A list of point of sale device assets is confirmed to exist that only includes device assets that are subject to version 3.1 compliance verification checks. (see URL below)

www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Observation

The 2015 payment card industry data security standard (version 3.1) requirements mandates that:

- a) (2.1) Vendor-supplied default accounts and passwords should be changed, removed or disabled. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).
- b) (9.9) policies and procedures require that a list of all POS (Point of Sale) or POI (Point of Interaction) device assets exist. Requirement 9.9.1.further states that the inventory list of devices is maintained as up-to-date and includes the following information:
 - Make, model of device;
 - Location of device (for example, the address of the site or facility where the device is located); and
 - Device serial number or other method of unique identification.

Discussions and examination of records identified that:

- a) Although a well defined and PCI-DSS compliant password policy is in place the security penetration tests have found weak passwords in use and the default admin name has not been changed; and
- b) A list of the point of sale device assets was unavailable for examination at the time of the audit to enable the list to be verified as containing only devices that meet the PCI: DSS ver3.1 requirements.

There is an increased risk of non-compliance until

- a) passwords and default accounts are confirmed as compliant; and
- b) A list of point of sale device assets is confirmed to exist that only includes compliant devices.

Responsibility

Information Security Manager

Management response / deadline

- a) Recommendations made by the external security test teams and documented in our remedial action plan (R.A.P) have now been applied and approved by Cabinet Office as part of our PSN submission – awarded 2nd November 2015
- b) Asset Register for point of sale devices will be created by 15th March 2016





Recommendation 4: Capita Services PCI DSS compliance verification status (Priority 3)

<p>Recommendation</p> <p>The Council should request documentary evidence to help demonstrate the extent to which the authority can place dependence on its third party service provider's compliance to the PCI DSS requirements.</p>
<p>Observation</p> <p>The "Dependence on another service provider's compliance" section (page 6) of the 2015 payment card industry data security standard PCI-DSS (PCI DSS Compliance Template for use with PCI DSS v3.1, Revision 1.0) states there is no need to force the third-party service provider to be assessed against PCI DSS 3.1 while their PCI DSS 2.0 assessment is still valid but the extent of their current PCI DSS compliance should be documented.</p> <p>Documentary evidence to demonstrate the extent to which the authority can place dependence on its third party service provider's compliance was unavailable for examination at the time of the audit.</p> <p>There is an increased potential risk of non-compliance until evidence is provided to demonstrate the extent to which the Council can depend upon its third party service provider's compliance.</p>
<p>Responsibility</p> <p>Information Security Manager</p>
<p>Management response / deadline</p> <p>Information Security Manager will request supplier evidence and review.</p> <ul style="list-style-type: none"> • Request evidence from third party suppliers by 31st December 2015 • Review evidence provided by 31st January 2016 • Recommendations {if applicable} (to supplier) by 15th February 2016 <p>Review the application of recommendations by supplier –by 31st March 2016</p>

Appendix A - Reporting Definitions

Audit assessment

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used:

Level	Symbol	Evaluation Assessment	Testing Assessment
Full		There is a sound system of internal control designed to achieve the system objectives.	The controls are being consistently applied.
Substantial		Whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk.	There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
Limited		Weaknesses in the system of internal control design are such as to put the system objectives at risk.	The level of non-compliance puts the system objectives at risk.
Nil		Control is generally weak leaving the system open to significant error or abuse.	Significant non-compliance with basic controls leaves the system open to error or abuse.

The assessment gradings provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Full' does not imply that there are no risks to the stated control objectives.

Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Level	Definition
Priority 1	Recommendations which are fundamental to the system and upon which the organisation should take immediate action.
Priority 2	Recommendations which, although not fundamental to the system, provide scope for improvements to be made.
Priority 3	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.
System Improvement Opportunity	Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

Appendix B - Staff Interviewed

The following personnel were consulted:

- John Worts - Information Security Manager
- Robbie File – Business Systems Developer
- Amanda Jeffries - Service Desk Lead Officer ICT Services

We would like to thank the staff involved for their co-operation during the audit.

Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by us should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Our procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our work and to ensure the authenticity of such material. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Mazars Public Sector Internal Audit Limited

London

December 2015

This document is confidential and prepared solely for your information. Therefore you should not, without our prior written consent, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. No other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

In this document references to Mazars are references to Mazars Public Sector Internal Audit Limited.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 4585162.

Mazars Public Sector Internal Audit Limited is a subsidiary of Mazars LLP. Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.