Project 'PCI Compliance'

End of Project Review

Document: PCI project Review
Issue Date: 8th February 2010
Version: 1.0

Change Control

Quality Assurance		
Document:	*PCI End of Project Review*	
Version:	1.0 (of the 4th January 2010)	
Status:	Draft	
	Name	**Date**
Document Owner:	Simon Stubbs	08/02/2010
Prepared by:	Simon Stubbs	08/02/2010
Verified by:	Kevin Rump	
Approved by:	Kevin Rump	
Final Authorisation:		

Circulation and Accreditation List				
Ver.	**Status**	**Date**	**Name**	**Organisation/Position**
0.1	Initial Draft	04/01/2010	Simon Stubbs	ICT Project Manager

Changes to Log				
Ver.	**Status**	**Changed by**	**Date**	**Events**
0.1	Initial Draft	Simon Stubbs	04/01/2010	Initial creation & draft
0.2	Updated Draft	Simon Stubbs	10/01/2010	Updated Draft
0.3	Updated Draft	Simon Stubbs	21/01/2010	Updated Draft
1.0	Final Release	Simon Stubbs	08/02/2010	Final Release

Purpose

To review the outcome of the project in relation to the project initiation document. The review takes into account any costs, schedules and tolerances.

The primary use of this document is to form the basis of any future work in terms of Payment Card Industry (PCI) compliance for Breckland Council.

Composition

The review takes into account the current situation in terms of how Breckland Council compares with the PCI Data Security Standard (DSS) version 1.2.1.

The report aims to cover the cores areas;

- Achievements of the PCI projects objectives.
- Review of benefits to date (if any).
- Performance against the planned target date, cost and tolerances.
- How could compliance be achieved /post project review plan.

Contents

1 Executive Summary

1.1. Summary

The PCI Compliance project was tasked with assessing the current Breckland Council status in relation to the PCI DSS standard 1.2.1 (dated July 2009). The PCI standard consists of twelve main requirement sections with these twelve sections further grouped into six main categories. Compliance on all elements is required to achieve full PCI DSS accreditation. Currently Breckland Council would achieve around 40% compliance against the current standard if formally assessed. This compliance figure is relatively low due in main to having an on site, non managed APCS system, lack of network segregation (restricting ability to control / segregate internal data traffic), lack of formal documented procedures and policies together with an open approach to how card payments are accepted within Breckland Council. Based on the findings Breckland Council would need to make a number of significant changes to internal infrastructure, technology and policy to achieve PCI compliance.

2 Background

2.1. Introduction

Breckland Council currently accepts debit card payments from members of the public to pay for services which are provided by the Council. At the present time no credit card payments are accepted as Breckland Council does not have compliance with the PCI DSS. The PCI DSS was developed to raise awareness and improve security across the board in the way payment card details are stored and processed. While the standard is not enforceable under law there is a contractual obligation enforced by substantial fines and the risk of adverse publicity should credit card details be made public as a result of a failure by Breckland Council. Currently Breckland Council stores /

processes card information on site so the PCI DSS needs to be addressed if credit card payments are to be accepted in the future. In order to achieve compliance Breckland Council would need to assess the current Breckland Council environment against the latest PCI DSS standard and achieve 100% compliance before accepting credit card payments.

3 Current environment

3.1. Existing payment environment

Breckland Council currently accept debit card payments in five main streams, Touchtone (automated phone payment system), Web / Internet, in person Chip & Pin, through the Call Centre and Backoffice (see appendix 1). The Touchtone and Web / Internet payments are handled by a fully managed APACS system managed by Capita. The Chip & Pin system whilst utilising the managed APACS system does also interface to the AIM database on site at Breckland Council's Elizabeth House location. The Call Centre and Backoffice both utilise an onsite APACS system (supplied, but not fully managed by, Capita). Any payments made via the Touchtone or Internet is handled by Capita and does not "touch" the Breckland Council environment when payment is made. The contact centre and onsite Backoffice both utilise the PAYe.net system which interfaces to an onsite APACS and the AIM database.

3.2. Non-Breckland payments

Companies who are contracted by Breckland Council to provide services do accept credit card payments (what about debit cards?). As part of the PCI compliance assessment these companies should also be assessed to ensure PCI compliant. Serco provide both bulk waste

and green bin services direct to the public and as such accept credit card payment for these services. The monies received from the public for these services are transferred from Serco to Breckland Council. Serco have confirmed that they are currently compliant with the PCI DSS standard. (Follow up action will be to obtain evidence – maybe from PCI)

4 PCI DSS Assessment Procedure

4.1. PCI DSS Assessment Process

The PCI DSS standard, version 1.2.1, was used to perform the assessment of the existing Breckland Council environment. The PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The *PCI Data Security Standard Requirements and Security Assessment Procedures,* uses as its foundation the 12 PCI DSS requirements (see appendix 2), and combines them with corresponding testing procedures into a security assessment toolkit.

4.2 *Assessment toolkit*

The PCI DSS assessment tool kit has been utilised for the Breckland Council PCI assessment. The assessment toolkit comprises of a checklist with twelve requirements. Each requirement comprising of individual elements with testing procedures, confirmation if in compliance or not along with a comment (if applicable). Each of the twelve requirements of the PCI DSS has varying numbers of elements, ranging from three to thirty nine and in total there are two hundred and seven individual elements which require satisfying to achieve accreditation to the PCI DSS standard. In order to assess the current status of Breckland Council against the PCI DSS each individual element from each of the twelve requirements was assessed against the testing procedure. For each individual element the requirement is either “In Place” or “Not in Place” which is signified by a “Y” or “N”. Further more for each element additional information is provided in the

"Comments" section. Due to this report being a preliminary investigation / assessment there are instances where due either to the ambiguity of the question or through lack of knowledge the answer is not clear, in such instances the compliance is set to "Not in Place". For each of the twelve sections a percentage of compliance is generated and as such an overall compliance percentage figure is created. In this way a metric of overall compliance is possible.

4.3 PCI DSS Results Matirx

Appendix 3 shows the 12 PCI DSS requirements and their corresponding individual elements. Each requirement is focussed on a particular area of security.

4.1.1. Build and maintain a secure network

Requirements one and two primarily focus on firewalls, boundary security and secure system configuration. The current security measures in place are lacking when compared to the requirements of the standard for this requirement. There is a need to achieve additional work on documentation to formalise the procedures and policies which are currently verbally in place. Additionally a reduction in scope of infrastructure under review would also significantly assist achieving compliance in this area. To achieve this reduction in scope the officers currently able to accept and process card payments would need to be considered carefully along with how the network infrastructure / topology is designed.

4.1.2. Protect cardholder data

Requirements three and four deal with protecting stored cardholder data and encryption of transmitted data across open public networks. Requirement three is mainly dealing with how card holder data is stored. As with requirements one and two the need to provide documented evidence is currently lacking which greatly weakens the ability to achieve compliance. The

majority of requirement four deals with cryptographic data transmission, currently it is unclear if the systems in place meet this requirement (further discussion with Capita would need to address this issue).

4.1.3. Maintain a vulnerability management program

Requirement five deals purely with the implementation, configuration and use of antivirus products. Requirement five is fully meet and as such requires no additional attention. Requirement six is primarily concentrating on how to develop and maintain secure systems and applications. Many of elements are specifically aimed at ensuring that the card payment systems in use are developed in line with best practice guidelines (PA DSS and Open Web Application Security Project OWASP), this being the case the majority of the elements will require consultation with Capita due to the bulk of this requirement relating to payment websites).

4.1.4. Implement strong access control measures

Requirement seven deals with restricting access to cardholder data and when access is granted it is on a least permissions basis first. The majority of requirement seven requires strong documented evidence that the controls and procedures are in place and enforced (as with other requirements under review this area needs addressing within Breckland Council to achieve compliance as documented procedures and policies are currently weak). Requirement eights intention is to ensure assess controls are in place and every users access can be traced. The requirement is only partial achieved by the current Breckland environment and additional work is necessary to achieve full compliance in this respect, primarily in the way access is granted initially, how user accounts are disabled and access rights granted. Requirement nine is tasked with

assessing how physical security is handled. The results from the assessment shows that Breckland Council meets approximately two thirds of the elements of the requirement with further work required in the security and control of both electronic and paper media used to store card holder data.

4.1.5. Regularly monitor and test networks

Requirement ten is focussed with monitoring access to networks and resources. Logging does take place within Breckland Council on the systems in question but the level and depth of logging is not clear in relation to the requirement. The indication is that additional and more detailed logging will be necessary to fully meet the compliance required. Additionally more work on documenting procedures is required. Requirement eleven deals with testing of security systems and the processes which are in place. Currently additional technological solutions would be required to achieve compliance in this requirement; this would include internal and external quarterly scanning and improved file integrity checking tools.

4.1.6. Maintain an information security policy

Requirement twelve is concerned with how internal security policies address information security for employee's and external parties (contractors). This requirement is heavily dependant on proof of documentation which accounts for the poor score achieved by Breckland Council against this requirement. Considerable work on documentation and user education would be required to achieve compliance against this requirement.

4.2. PCI DSS High Level Results

Appendix 4 shows the summary table from the PCI DSS results matrix. Only requirement five (use and regularly update anti-virus software) is currently fully compliant with the PCI DSS 1.2.1. Requirements four, eight and nine are partially compliant with the remaining requirements needing considerable work to reach the full compliance stage. Appendix 5 uses a radar chart to indicate areas of strength and weakness in the current assessment against each requirement.

5 Summary

5.1. Summary

The findings of the initial PCI DSS assessment are that the current Breckland Council environment is approximately 40% compliant against the PCI DSS version 1.2.1. There would appear to be a number of reasons for the low compliance score;

5.1.1 Onsite APACS

Utilisation of both a fully managed and onsite APACS system (this situation is apparently quite unusual). The onsite APACS is not fully managed by Capita (Steria carry out the day to day administration and updates). This onsite APACS would appear not to be PCI compliant. (Certainly agree)

5.1.2 Network segregation

Lack of physical network segregation on the Breckland Council network. The inability to restrict internal traffic on the data network from those areas within Breckland Council which utilise card payment systems will increase the scope of the network included in the PCI compliance. Consideration must be given to reducing the need to allow payment card details from flowing across the entire Breckland.

5.1.3 Documentation

Major lack of documented policies and standard operating procedures (SOP) in relation to the way card holder data is processed within Breckland Council. Much of the PCI DSS requires documented proof of the procedures and policies which are in place. Failure to provide documented evidence, even if the requirement is in force prevents compliance being achieved.

5.1.4 Paper based systems

Ability of Backoffice service areas to receive and process paper based card details. The lack of control in relation to paper based card information passing through the Breckland Council offices causes a number of issues in achieving compliance due mainly to the lack of control of this media.

6 Recommendation

6.1 Recommendations

The following recommendations are provided as the basis for any project looking at achieving PCI DSS compliance.

6.1.1 Scope of project

The main factor to consider in a future PCI compliance project would be to identify the scope of the works required. Restricting the scope of the PCI DSS review would have significant benefits in terms of achieving compliance. Review how card holder data is processed

within Breckland Council currently, in particular the areas which can process card payment details. Any reduction in the amount of people and services involved in the card payment process would have the advantage of reducing scope for a future compliance project.

6.1.2 APACS

Discussions with Capita would need to take place over how best to remove the onsite APACS and utilise a fully managed APACS or how to achieve PCI compliance with the onsite APACS (if possible).

6.1.3 Network infrastructure

Given the flat structure of the Breckland Council network any future PCI compliance project will need to consider methods of network segregation to allow far more control of how internal card data is passed around the Breckland data network. The ability to restrict card data within the Breckland data network and in particular provide evidence as to how the payment card data is managed is important to allow compliance to be achieved.

.

6.1.4 Documentation

Instigate a program to create standard operating procedures and fully document how the payment card environment operates within Breckland Council. Any future compliance project will need this information in place to successfully achieve compliance as a great deal of the standard requires documented evidence to the support the application.

6.1.5 Ownership

Ensure there is clear ownership of the payment card environment within Breckland Council. Currently there does not seem to be an overall authority within Breckland Council responsible for the card payment system.

6.1.6 External Assistance

It is clear from the assessment carried out that the PCI DSS standard is open to interpretation in certain areas and some elements are slightly ambiguous in nature. The assistance of a PCI consultant to assist Breckland Council in the early stages of any formal PCI compliance project would certainly be recommended. Likewise should a formal decision be made to achieve PCI compliance engaging with Capita at an early stage would be a necessity.

7 Project statistics

7.1 ***Project achievements***

The PCI DSS assessment has identified how the achievement of PCI compliance would be obtained and delivered a metric clearly quantifying the current status of Breckland Council against the PCI DSS standard through the use of a PCI DSS assessment matrix.

7.2 Project Tolerances

In terms of the project tolerances these can be assessed as follows;

7.2.1 Time

Time: Must deliver the review of the assessment by Jan 2010. The project information gathering and assessment matrix was completed within the allocated time scale however the final end of project report was delivered after the deadline.

7.2.2 Cost

Cost: There is no budget for the assessment stage. As the project did not have any budget assigned and the work was primarily a research tasks no costs have been incurred during the project lifecycle.

7.2.3 Scope

The scope of the works was to complete the preliminary assessment stage of the PCI DSS only. This has been achieved.

7.2.4 Quality

Quality: Normal business operations should not be affected. At no point has the operation of Breckland Council been affected by the PCI DSS assessment project.

7.2.5 Risks

Risk: All high likelihood/high impact risks to be escalated. At no point during the assessment where any risks identified which would require escalating.

7.2.6 Benefits

Benefits: no tolerance set. The projects main benefit is in providing a starting point for any future PCI compliance project.

7.3 Risks & Issues

During the prilimary PCI DSS assessment a number of risks and issues where identified. The have been categorised as follows;

7.3.1 Issues

Total Issues raised to Date:	4			
	New	**Pending**	**Closed**	**Total**
Top (see below)	0	0	0	**0**
High	0	0	0	**0**
Medium	4	0	0	**4**
Low	0	0	0	**0**
Total	4	0	0	**4**

7.3.2 By issue Type

	Raised to date
Request for change	**0**
Off Specification	**0**
General Questions	**0**
Statement of Concern	**4**

7.3.3 "Highest" Issues

ID	**Brief Issue Description**
1	Due to the lack of network segregation the compliance assessment work will probably need to consider the entire Breckland network infrastructure.
2	Lack of documented policies for the card payment system
3	Lack of in house knowledge on PCI compliance
4	Current onsite APACS system not PCI compliant.

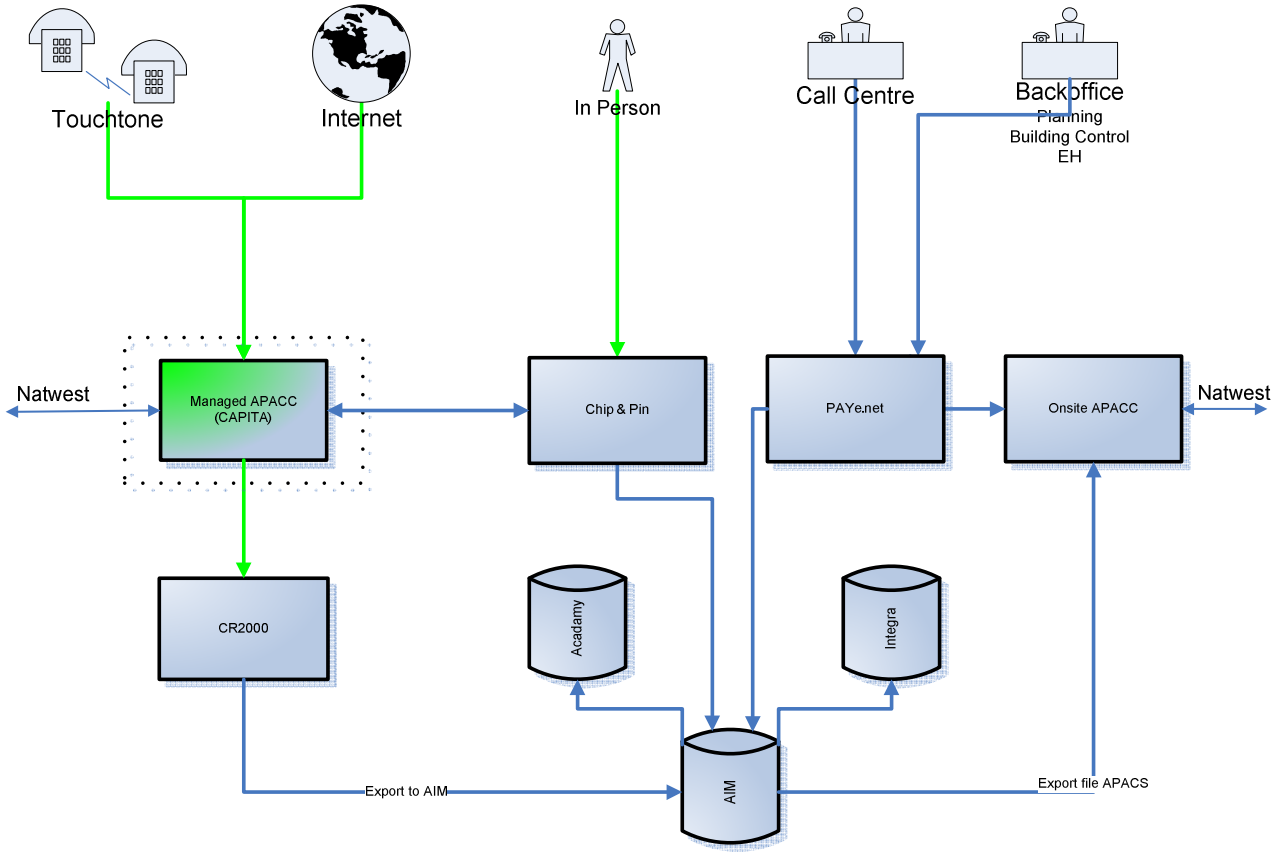
7.3.4 Risk Summary

Total Risk identified to date:					7
Probability	**No Change**	**Reducing**	**Increasing**	**Closed**	**Total**
High	5	0	0	0	**5**
Medium	2	0	0	0	**2**
Low	0	0	0	0	**0**
Total	7	0	0	0	**7**

7.3.5 "Highest" Risks

ID	Brief Risk Description
1	Failure to obtain PCI compliance would lead to Breckland Council not being able to allow credit cards to be used for payment of services.
2	Lack of documentation for current procedures within the card payment system.
3	Should the standard version change between assessment and compliance then the assessment stage would need to be completed again.
4	Serco might not be PCI DSS compliant and as such would mean Breckland Council could not obtain compliance for the full services offered by card payment.

Appendix 1



High level card payment over view

November 2009 – Rev 0.3

Appendix 2

PCI Data Security Standard – High-Level Overview

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

Appendix 3

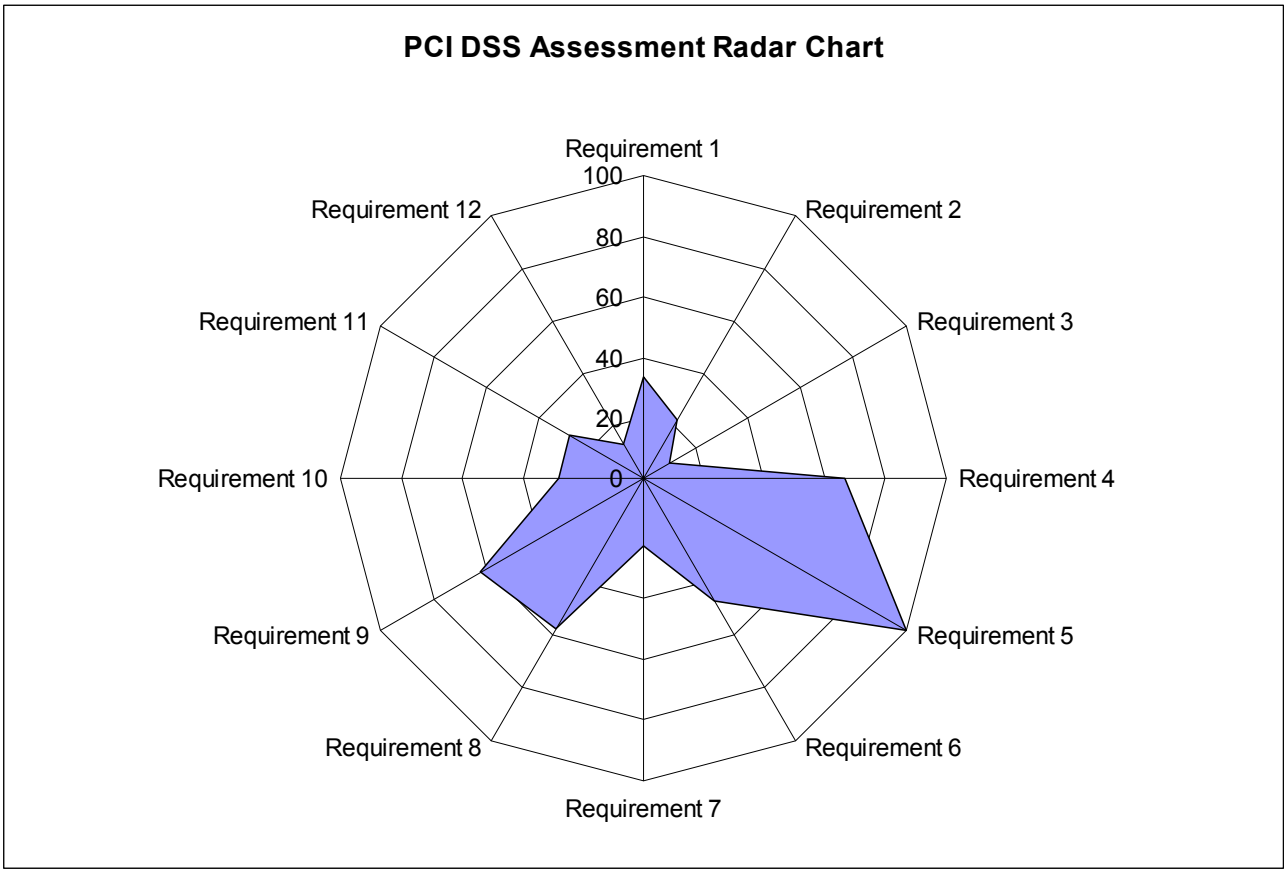
Appendix 3 relates to the PCI DSS compliance Matrix. The following link will load the matrix. The summary sheet provides and overview of the compliance with each tab relating to a separate requirement.

PCI DSS Assessment Matrix\MASTER PCI DSS Assessment Matrix v3.xls

Appendix 4

Category	Percentage in Place (%)	Percentage to Complete (%)	Current Status
Requirement 1	33	67	Non-compliant
Requirement 2	22	78	Non-compliant
Requirement 3	10	90	Non-compliant
Requirement 4	67	33	Non-compliant
Requirement 5	100	0	Fully compliant
Requirement 6	47	53	Non-compliant
Requirement 7	22	78	Non-compliant
Requirement 8	57	43	Non-compliant
Requirement 9	62	38	Non-compliant
Requirement 10	28	72	Non-compliant
Requirement 11	29	71	Non-compliant
Requirement 12	13	87	Non-compliant
Overall Compliance	40.81	59.17	Non-compliant

Appendix 5


PCI DSS Assessment Radar Chart
Requirement 1
100
80
60
40
20
0
Requirement 2
Requirement 3
Requirement 4
Requirement 5
Requirement 6
Requirement 7
Requirement 8
Requirement 9
Requirement 10
Requirement 11
Requirement 12