Warwick District Council

ICT Steering Group – PCI DSS Compliance centralised logging system

Digital services so good that people prefer to use them

WARWICK DISTRICT COUNCIL

www.warwickdc.gov.uk

ICT Steering Group – PCI DSS Logging System Business Case

Revision History

Document	ICT Steering Group – PCI DSS Logging System Business Case
Author	Tass Smith
Date Completed	27 January 2017
Reviewed Date	

Version	Revision Date	Revised By	Revisions Made
0.1	27 January 2017	Tass Smith	Final document
0.2			
1.0			
2.0			
3.0			
4.0			

Approvals

This document requires the following approvals:

Title
ICT Steering Group

Distribution

This document has been distributed to:

Name	Title

Contents

ICT Steering Group – PCI DSS Logging System Business Case 2
1 Business Problem Analysis 4
1.1 Business Problem 4
2 Preferred Solution 5
2.1.1 PCI DSS Compliance Logging System 5
2.1.2 Benefits, Goals and Measurement Criteria 5
2.1.3 Digital Benefits 5
2.1.4 Costs and Funding Plan 6
2.1.5 Risks 7
2.1.6 Issues 7
2.1.7 Assumptions 7
3 Implementation Approach 8
3.1 Outline Project Scope 8
3.2 Service Area Resources 8
3.3 ICT Services Resources 8

1 Business Problem Analysis

This section seeks to describe the issue to be addressed by the project. It consists of two parts, Business Problem and Business Opportunity. When completing this section is advisable to only complete one section depending on whether you are trying to resolve an existing problem or are looking at a new opportunity. For example, a new income generation scheme would be a business opportunity rather than a business problem.

1.1 Business Problem

Warwick District Council (WDC) receives customer debit and credit card payments via “point of sale” card terminals, by phone and via online (web based) payment systems. The Payment Card Industry Security Standards Council have mandated that all card merchants, of which the Council is one, must become compliant with their Data Security Standard (PCI DSS) to continue to receive card payments.

WDC are being ‘fined’ around £10,000 per year by HSBC (one of our acquiring banks) because we are non-compliant. To achieve compliance, WDC needs to complete some Self-Assessment Questionnaires to declare that we are meeting all the relevant criteria. The latest PCI DSS standard is more stringent than previous versions and we are required to provide evidence that our card terminals are subject to regular anti-tampering checks and that all staff have received relevant and regular training, amongst other things.

We would like to create a PCI DSS Logging System to make it easier to monitor these checks / training requirements and to make ongoing compliance easier to maintain.

2 Preferred Solution

This section provides details of the Service Area's preferred solution, its benefits, costs, feasibility, risks and issues.

2.1.1 PCI DSS Compliance Logging System

A database with an internal web front-end which would hold a centralized log of:

- Card terminals
- Anti-tampering checks
- Staff Training
- Service Provider Compliance

Also, we would have a couple of TotalMobile forms to capture the initial card terminal installation and subsequent anti-tampering checks. Using TotalMobile would allow all inspection results (including photographs) to be automatically uploaded to the database.

The database would be linked to Active Directory to ensure that staff moving into / away from card processing roles would receive relevant (refresher) training in a timely manner.

2.1.2 Benefits, Goals and Measurement Criteria

Describe the tangible and intangible benefits to the Service Area upon implementation of the solution. One of the obvious benefits described will be that the business problem / opportunity outlined above will be addressed.

NB: The benefits listed below are examples only and the boxes should be modified to describe the project's actual benefits. All quantifiable benefits listed must be supported by current performance figures.

Complete the following table:

Category	Benefit	Value
Financial	Cost reductions	Saving around £10,000 per year in HSBC non-compliance fines
Operational	Compliance would be easier to maintain and audit	Regular anti-tampering checks could be carried out with ease and minimal back office intervention Audit checks could be carried out easily, making ongoing annual compliance easier to evidence
Customer	Customers would be reassured that their card payments are protected by our PCI DSS Compliance	Corporate reputation would be maintained, leading to consistent or increased customer card payments.
Staff	Staff would be protected from risks associated with poor compliance regime	Staff would receive their initial and refresher training in a timely manner Staff would be able to add / remove Chip & Pin devices from the estate with relative ease.

2.1.3 Digital Benefits

Description	Value

How many citizens will the project benefit? *For example, does the project only benefit council tenants, people with parking permits or users of one of our facilities? Where theoretically a service could be used by anyone in the district, actual usage figures should be used.*	Potentially every citizen / business that's required to make payments to WDC
How many transactions does the business process deal with? *For example, a particular business process may have 5,000 customers annually, but as they are required to contact the service quarterly, they therefore generate 20,000 transactions annually.*	??
What is the average current duration of the process from service request to completion?	Time to make card payments won't be affected. However, the time spent proving our PCI DSS Compliance will be vastly reduced.

2.1.4 Costs and Funding Plan

Capital Costs	Amount
• Initial software purchase – not required • Data gathering – not required • New hardware – propose to use hand held devices from H&PS (1 only) • Temporary additional resources - not required	N/A (we already own the TotalMobile platform) Mobile device cost around £300 each
Total	
Revenue Costs	**Amount**
• TotalMobile Software license costs for **1** users (could be £0 if we are able to re-use 1 of H&PS existing licenses)	£750 per licensed user (one off cost)
• TotalMobile Support costs for **1** users – reduced price if we can re-use one of H&PS licenses (could be £150 in total if we can re-use 1 of H&PS existing licenses which are based on 10% of the license price)	£150 per license per year (20% of license price)
• Mobile device and data contract x 1 users	(Devices cost £295.21 each)when connected to O2's 3g network with 3Gb data for £9.00 per month on a 24 month contract.
Total	**Max £1045.21 per user one off cost** **£258 per user annually**

For both the capital and revenue amounts identified above, please indicate how the funding will be made available.

Funding Source	Amount	Notes
Licence costs – Existing Corporate PCI DSS Compliance budget	£9/month	*Depends on which Service Area 'owns' PCI DSS Compliance*
One off costs – Existing Corporate PCI DSS Compliance budget	£1045 per user	*May be £0 if we can re-use existing TotalMobile devices / licences*

2.1.5 Risks

Summarise the most apparent risks associated with the adoption of this solution.

Description	Likelihood (1 – 5)	Impact (1 – 5)	Mitigating Actions
That the solution isn't fit for purpose and WDC is not able to easily evidence PCI DSS Compliance at its annual review	2	5	That the project requirements are correctly specified, developed and tested with reference to the current PCI DSS version. Any proposed PCI DSS version changes are monitored in case scope changes are required.
That the solution isn't ready on schedule and the HSBC fines continue to be charged	2	4	That sufficient project resource is made available to specify, develop, test and implement the solution

To complete this section thoroughly, it may be necessary to undertake a formal Risk Assessment. To reduce the likelihood and impact of each risk occurring, clear 'mitigating actions' should be defined.

2.1.6 Issues

Summarise the highest priority issues associated with the adoption of this solution

No.	Issue - Description
1.	That sufficient resource is made available to this project and subsequent compliance process

2.1.7 Assumptions

List the major assumptions associated with the adoption of this option.

No.	Assumption - Description
1.	That the proposed solution satisfies the PCI DSS Compliance requirements

3 Implementation Approach

This section not only requires the service area to understand its business objectives, but to clearly understand the scope of the activity. In doing so, consideration should be given to the 'digital design principles'. Special consideration should be given to whether all the customer transactions for a specific process should be in scope. For example, if a process deals with 10,000 transactions annually, of which 8,000 are identified as easy to deal with, then perhaps this is sufficient for the scope of the project.

3.1 Outline Project Scope

- Create an Intranet-based web front end Logging System
- System to store:
    - all training documentation
    - lists of staff who require relevant training and to log the training they've received
    - lists of live Chip & Pin devices
    - anti-tampering checks for each device
    - third-party service provide PCI DSS Compliance certification
- System reports to enable audits of above data
- TotalMobile forms developed for the initial and subsequent anti-tampering checks
- TotalMobile integration needed to the PCI DSS Logging System
- No further integration is required to other systems

3.2 Service Area Resources

Please use this section to describe how the service area is going to produce the necessary capacity to deliver the project.

- Project manager – To be decided (depends who owns it) but Tass Smith initially
- Design authority – Graham Folkes-Skinner / David Adcock
- Testing - Graham Folkes-Skinner
- Training – Service area staff & system owner (depends who owns it)
- System owner – to be decided

3.3 ICT Services Resources

This section should be used to describe the resource to be provided by ICT Services. To do so, the service area sponsor will need to meet with the ICT Services Applications Support Manager to agree the project scope and likely method of approach.

- Apps Support Analyst with TotalMobile experience
- Apps Support Manager
- Business Analyst