**Change Management Process**

**Questionnaire**

UBC PCI DSS

The University of British Columbia

Table of Contents

[Introduction 3](#_Toc379457284)

[Scope 3](#_Toc379457285)

[PCI DSS Deliverables 4](#_Toc379457286)

[Change management questionnaire 5](#_Toc379457287)

[Section 1. Identify the change 5](#_Toc379457288)

[Section 2. Hardware/software specifications, testing and training 6](#_Toc379457289)

[Section 3. Security and systems stability 7](#_Toc379457290)

[Section 4. Tracking, reporting and closure of change 7](#_Toc379457291)

[Section 5. UBC standards 8](#_Toc379457292)

[Section 6. Sign Off 8](#_Toc379457293)

# Introduction

Change management process is an important process in every organization. The most critical success factor in change management process is that merchants understand and have properly documented their cardholder data environment[[1]](#footnote-1) (CDE).

The main objective of this document is to document the change activity that has possible impact to CDE, and PCI DSS compliance. The change management process needs to address both technical and business process changes affecting credit card processing and its compliance with PCI DSS requirements.

Without knowing how the CDE operates and functions, merchants will encounter difficulty of figuring out the effect of the change to the existing and/or new CDE. This questionnaire will provide a minimum guide to manage changes that will be made to the CDE and is not a substitute to a formal change technical feasibility and change impact analysis; and to ensure that PCI DSS requirements are always taken into account before, during and after implementation of the change.

# Scope

Apply to change(s) made in CDE and business process and its impact to PCI DSS requirements.

# PCI DSS Deliverables

* Merchants should submit the change management questionnaires to Revenue Accounting (c/o Raul Ramos – rramos@mail.ubc.ca) together with updated business process documentation, i.e. CDE file and network diagram.
* Changes to the CDE should be approved by the system owner after consultation with the systems administrator responsible for the system. The PCI Working Committee’s technical and security resources are available for consultation if there are any questions on PCI compliance.
* Depending on the complexity of the change in the CDE, merchants are requested to seek the professional advice of a Qualified Security Assessor (QSA) to ensure that all changes are in compliance to PCI DSS policy and requirements.
* Contact Raul Ramos to facilitate the discussion with either the PCI Technical Resource or the QSA. The QSA will require the network diagram of the credit card flow process to determine change in current SAQ level.
* Complete the appropriate SAQ[[2]](#footnote-2) form if the current SAQ level will change due to the implemented change in the system and/or business process.
* Both external and internal scans are required after any significant change in the network is made.

# Change management questionnaire

|  |  |
| --- | --- |
| Merchant Name: |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Require change to cardholder data environment (CDE) and/or business process | Yes |  | No |  |

|  |  |  |  |
| --- | --- | --- | --- |
| SAQ Level Before the Project: |  | Expected SAQ Level After the Project: |  |
| Classification of Change: | Significant[[3]](#footnote-3) |  | Not Significant |  |

## Section 1. Identify the change

|  |  |
| --- | --- |
| 1. | Describe the change and business justification? |
| *Please provide details:* |
|  |
|  |
|  |

|  |  |
| --- | --- |
| 2. | Who requested the change? |
| *Please provide details:* |
|  |

|  |  |
| --- | --- |
| 3. | Who approved the change? |
| *Please provide details:* |
|  |

|  |  |
| --- | --- |
| 4. | Will the change affect the CDE and/or the credit card business process? |
| *Please provide details:* | Yes: |  | No: |  | Not Applicable: |  |
|  |

|  |  |
| --- | --- |
| 5. | Do you require the assessment of a QSA to ensure that the change comply with PCI DSS1 requirements? |
| *Please provide details:* | Yes: |  | No: |  | Not Applicable: |  |
|  |

## Section 2. Hardware/software specifications, testing and training

|  |  |
| --- | --- |
| 6. | What PCI DSS requirement(s) is (are) directly impacted as a result of this change? |
| *Please provide details on the impacted PCI Requirement(s):* |  |  |  |  |  |  |
|  |
|  |
|  |

|  |  |
| --- | --- |
| 7. | What is the name of the hardware/device or payment application/software solution you will use? |
| *Please provide details:* |  |  |  |  |  |  |
|  |

|  |  |
| --- | --- |
| 8. | Is the Service Provider of the hardware/device or software solution PCI DS compliant? |
| *Please provide/attach documentation:* | Yes: |  | No: |  | Not Applicable: |  |
|  |

|  |  |
| --- | --- |
| 9. | Is the hardware/device or payment application/software solution PTS[[4]](#footnote-4) and/or PA DSS[[5]](#footnote-5) compliant? |
| *Please provide explanation:* | Yes: |  | No: |  | Not Applicable: |  |
|  |

|  |  |
| --- | --- |
| 10. | Do you envision there will be a need for end user training? |
| *Please provide details of the type of training and who will be supplying the materials.* | Yes: |  | No: |  | Not Applicable: |  |
|  |

## Section 3. Security

|  |  |
| --- | --- |
| 11. | Is the new/replacement hardware/device or payment application/software solution storing customer’s Primary Account Number[[6]](#footnote-6) (PAN)? |
| *Please , provide information on steps to be taken to ensure appropriate security and PCI compliance are applied:* | Yes: |  | No: |  | Not Applicable: |  |
|  |
|  |

|  |  |
| --- | --- |
| 12. | Is the Service Provider storing personal information outside Canada? |
| *Please provide information on data types and steps identified to ensure confidentiality:* | Yes: |  | No: |  | Not Applicable: |  |
|  |
|  |

## Section 4. Tracking, reporting and closure of change

|  |  |
| --- | --- |
| 13. | Are the approved changes and PCI requirements implemented as planned? |
| *Please provide information:* | Yes: |  | No: |  | Not Applicable: |  |
|  |

|  |  |
| --- | --- |
| 14. | Have you updated the associated system and user documentation and procedures relating to PCI requirements? |
| *Please provide information:* | Yes: |  | No: |  | Not Applicable: |  |
|  |  |  |  |  |  |  |

## Section 5. UBC standards

|  |  |
| --- | --- |
| 15. | Does the change comply with the Privacy policies on personal information set forth by the University? |
| *Please provide information:* | Yes: |  | No: |  | Not Applicable: |  |
|  |

|  |  |
| --- | --- |
| 16. | Do you confirm that the change address all required PCI DSS requirements? |
| *Please provide details:* | Yes: |  | No: |  | Not Applicable: |  |
|  |
|  |

## Section 6. Sign Off

|  |  |
| --- | --- |
|  | I attest that Choose Merchant Name complies with PCI DSS requirements in all aspects of the change. |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Signature of Merchant Head of Office |  | Date |
|  |  |  |
| Name of Merchant Head of Office |  |  |
|  |  |  |
| UBC Department/Centre/Unit |  |  |

1. Cardholder data environment is the area of computer system network that possess cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission (PCI SSC). [↑](#footnote-ref-1)
2. Self-Assessment Questionnaire is a validation tool for merchants and service providers that are not required to undergo an on-site data security assessment per the PCI DSS Security Assessment Procedures. The purpose of the SAQ is to assist organizations in self-evaluating compliance with PCI DSS (PCI SSC). [↑](#footnote-ref-2)
3. The determination of what constitutes a significant change is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the CDE, then it could be considered significant (PCI SSC). [↑](#footnote-ref-3)
4. The PIN Transaction Security relates to the capture, encryption, transmission and storage of cardholder PIN numbers and other account information. [↑](#footnote-ref-4)
5. The Payment Application Data Security Standards applies to software vendors and other who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties. [↑](#footnote-ref-5)
6. A PAN is the 16-digit number embossed, engraved, or imprinted on a payment card (Visa). [↑](#footnote-ref-6)