Western
UNIVERSITY · CANADA

Appendix A: Cloud-based Solutions and Accountabilities

Below are highlights from the Payment Card Industry (PCI) articulating important elements related to implementing a cloud-based solution utilizing payment services, but also apply to general considerations related to this type of hosting.

This appendix is included for all cloud-based solutions which also employ ecommerce to provide a context for all involved in terms of solution complexity, platform disposition, and mutual accountabilities.

Ensuring that cloud services are designed, maintained and used securely is a shared responsibility between the Provider and the Customer. It is important to note that all cloud services are not created equal. Clear policies and procedures should be agreed upon between the Customer and the Provider for all security requirements. Responsibilities for operation, management and reporting should be clearly defined and understood for each requirement and acknowledged, in writing, in contractual agreements.

Regarding third-party or public clouds, Customers should consider that while they can outsource the day-today operational management of the data environment, they retain responsibility for the data they put in the cloud.

The following steps should be followed by any organization looking to migrate to or evaluate cloud services:

- UNDERSTAND your risk and security requirements first.
- CHOOSE a deployment model that aligns with your and your industry's security and risk requirements.
- EVALUATE different service options.
- KNOW what you want from your Provider.
- COMPARE Providers and service offerings.
- ASK questions of the Provider and verify the responses; for example:
    - What does each service consist of exactly, and how is the service delivered?
    - What does the service provide with respect to security maintenance, PCI DSS compliance, segmentation and assurance, and for what is the Customer responsible?
    - How will the Provider provide ongoing evidence that security controls continue to be in place and are kept up to date?
    - What will the Provider commit to in writing?
    - Are other parties involved in the service delivery, security or support?
- DOCUMENT everything with your Provider in written agreements - for example, Service Level Agreements (SLAs)/Terms of Service contracts, etc.
- REQUEST written assurances that security controls will be in place, and periodic verification (e.g., compliance reports) that controls continue to be maintained.
- REVIEW the service and written agreements periodically to identify whether anything has changed.

If account data is stored, processed or transmitted in a cloud environment, PCI DSS will apply to that environment, and compliance will typically involve validation of both the Provider's environment and the Customer's usage of that environment.

Even though a Provider may claim to be PCI DSS compliant, the Customer should confirm that all the consumed services and locations were included in the Provider PCI DSS compliance validation, and that the services are used in a compliant manner.

Moreover, the allocation of responsibility between Customer and Provider for managing security controls does not exempt a Customer from the responsibility of ensuring that their cardholder data (CHD) is properly secured according to applicable PCI DSS requirements. Customers should define what PCI DSS requirements are shared among the Customer, Provider and any intermediaries (e.g., a payment gateway) and confirm their compliance.

There may be multiple layers or levels of Provider dependency, which can affect the security of the cardholder environment. Identifying all third-party relationships that the Provider has in place is important in order to understand the potential ramifications for a Customer's environment. The existence of multiple nested relationships will add complexity to both the Provider's and the Customer's PCI DSS assessment process.

Where the Customer has a direct contractual relationship with all nested Providers, the Customer will need to understand the impact.

As a general rule, the more aspects of a Customer's operations that the Provider manages, the more responsibility the Provider has for maintaining PCI DSS controls. However, outsourcing maintenance of controls is not the same as outsourcing responsibility for the data overall.

Where the Provider maintains responsibility for PCI DSS controls, the Customer is still responsible for monitoring the Provider's ongoing compliance for all applicable requirements. Providers should be able to provide their Customers with ongoing assurance that requirements are being met, and where the Provider is managing requirements on behalf of the Customer, it should have mechanisms in place to provide the Customer with the applicable records to demonstrate that the requires security controls are in place.