Section 06.05.05.02
PCI Compliance

All merchants and their service providers are required to comply with the Payment Card Industry Data Security Standard in its entirety. The PCI Data Security Standard Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS). There are several Self Assessment Questionnaire (SAQ) Validation categories, shown briefly in the table below. The table should be used to gauge which SAQ applies to your department. Each department accepting credit card payments must have a PCI Self Assessment Questionnaire on file with the Texas A&M University System Office and the Comptroller's Office. This form must be updated in May/June of each year and whenever a change takes place. Copies of blank Self Assessment Questionnaires can be found on the PCI Security Standards Council website at https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs.

Selecting the SAQ that Best Applies to Your Department

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No storage, processing, or transmission of cardholder data on merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: ▪ Imprint machines with no electronic cardholder data storage, and/or ▪ Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

SAQ	Description
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE	Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce merchants.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete an SAQ.