State of Arizona Accounting Manual

INTRODUCTION

SAAM 4016 described in general the Payment Card Industry Security Standards Council (hereinafter referred to as PCI) and the requirement for State agencies to comply with PCI Standards in order to continue to accept payment cards (i.e., credit cards, debit cards, charge cards, etc.) to collect money for taxes, licenses, other services and goods.

Compliance with PCI standards requires, among other things, an annual compliance audit. As part of that audit, vendors (i.e., agencies using payment cards to effect collections) must complete risk assessments. One of the risk assessments is IT related and the other deals with the operational environment not directly involving matters of information technology.

Since credit card contracts fall within the statutory jurisdiction of the Office of the State Treasurer (OST), it has overall responsibility for statewide PCI compliance. In matters relating to annual risk assessments, the OST works with the Arizona Strategic Enterprise Technology (ASET) and General Accounting Office (GAO) divisions of the Arizona Department of Administration.

This section of SAAM establishes the requirement to complete these risk assessments; it also directs agencies to tools that can be used to complete the risk assessments.

POLICY

1. Agencies that accept payment cards must annually complete two risk assessments.

1.1. The first risk assessment is the IT Risk Assessment.

1.1.1. Complete a formal PCI DSS compliant IT Risk Assessment to include an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30. Ensure that the IT Risk Assessment is in compliance with the PCI DSS Risk Assessment Guidelines published November 2012 and available online at: https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf

1.2. The second risk assessment is the PCI Non-IT Risk Matrix.

1.2.1. The PCI Non-IT Risk Matrix, Form GAO-PCI-1, can be found on the GAO Website at: https://gao.az.gov/publications/forms.

2. Both risk assessments must be completed annually not later than the last business day of September.

3. Either or both risk assessments should be completed more frequently than annually whenever there is a change in the IT or operational environment.

4. Risk assessments are to be retained by the preparing agency, but are to be made available upon request to the OST, ASET, the GAO or any PCI compliance auditor upon request.