CSU The California State University
OFFICE OF THE CHANCELLOR

Office of Audit and Advisory Services
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4210

Larry Mandel
Vice Chancellor and
Chief Audit Officer

562-951-4430
562-951-4955 (Fax)
lmandel@calstate.edu

February 24, 2016

Dr. Jane Close Conoley, President
California State University, Long Beach
1250 Bellflower Boulevard
Long Beach, CA 90840

Dear Dr. Conoley:

Subject: Audit Report 15-43, *Payment Card Processing*, California State University, Long Beach

We have completed an audit of *Payment Card Processing* as part of our 2015 Audit Plan, and the final report is attached for your reference. The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

I have reviewed the management response and have concluded that it appropriately addresses our recommendation. The management response has been incorporated into the final audit report, which has been posted to the Office of Audit and Advisory Services' website. We will follow-up on the implementation of corrective actions outlined in the response and determine whether additional action is required.

Any observations not included in this report were discussed with your staff at the informal exit conference and may be subject to follow-up.

I wish to express my appreciation for the cooperation extended by the campus personnel over the course of this review.

Sincerely,

Larry Mandel
Vice Chancellor and Chief Audit Officer

c: Timothy P. White, Chancellor

The California State University
Office of Audit and Advisory Services

PAYMENT CARD PROCESSING

California State University, Long Beach

Audit Report 15-43
January 5, 2016

EXECUTIVE SUMMARY

OBJECTIVE

The objectives of the audit were to review campus payment card processing activities to determine whether the campus had assessed the risks and exposures related to payment card processing and established a program to ensure compliance with applicable laws and payment card industry (PCI) regulations; and, if applicable, to ascertain the effectiveness of controls implemented to protect payment card information and adhere to PCI regulations.

CONCLUSION

Based upon the results of the work performed, except for the effect of the observations described below, the controls in effect as of October 9, 2015, taken as a whole, were sufficient to meet the objectives of this audit.

The controls and processes established over payment credit card processing at California State University, Long Beach (CSULB) included a written policy, governance structure, and formal risk assessment for credit card processing provided on campus. In addition, the campus had begun to assess future payment card processing requirements due in 2016 and had identified the controls required to meet PCI compliance. However, an opportunity exists to improve oversight and ensure that PCI attestation compliance is accurate.

Specific observations, recommendations, and management responses are detailed in the remainder of the report.

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. OVERSIGHT AND GOVERNANCE

OBSERVATION

The campus did not ensure that all PCI requirements were being adequately addressed and that new technologies implemented met PCI data security standards.

Specifically, the campus PCI policy designated responsibilities to various groups throughout the campus; however, there was no oversight designation to promote or ensure the quality, accuracy, and completeness of the overall campus PCI program.

As a result, we noted the following:

- Attestation documents prepared by some campus groups contained missing or conflicting information.
- Annual training on credit card processing was not provided to all campus groups.
- An electronic notebook without adequate security controls had been deployed for credit card processing.

RECOMMENDATION

We recommend that the auxiliaries assess the completeness and accuracy of their PCI attestations and that the campus enhance PCI oversight to include quality control responsibilities that assure campus management that the distributed PCI responsibilities are conducted sufficiently to satisfy PCI data security standards.

MANAGEMENT RESPONSE

The campus will establish a protocol whereby all campus and auxiliary attestations will be sent to the university chief financial officer. All attestations will be thoroughly reviewed for completeness, accuracy, and compliance with applicable standards. Attestations will be either formally accepted or returned to the user group for appropriate action.

Estimated date of completion is February 29, 2016.

GENERAL INFORMATION

BACKGROUND

The Integrated California State University Administrative Manual (ICSUAM) §8000, *Information Security Policy*, requires the California State University (CSU) to protect the confidentiality, integrity, and availability of CSU information assets and applies to all categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic).

In order to safeguard the personal information of individuals who hold credit cards, the five major payment card brands have endorsed the PCI Data Security Standard (DSS). The PCI Security Standards Council owns, develops, maintains, and distributes the PCI DSS. As a global standard, the PCI DSS applies to any entity worldwide that stores, processes, or transmits credit card-holder data. This includes financial institutions, merchants, and service providers in all payment channels.

Each payment card brand has PCI auditing and reporting requirements that merchant banks must meet in order to gain access to the payment network. The merchant banks must provide evidence that merchants using their bank, and any service providers used by those merchants, are PCI-compliant. This chain of liability at each level is designed to protect credit card-holder data by using PCI DSS to mitigate the risk of data breaches in the rapidly evolving threat landscape.

Although the PCI has defined compliance standards for data security, the CSU has not provided any specific guidance regarding oversight, governance, or assurance that annual compliance is achieved and maintained. It is the policy of the CSU that campuses be given the choice of credit card-processing vendors that best meet individual or unique campus hardware, service, and application requirements.

At CSULB, the information security office has primary oversight responsibility for credit card processing activities on campus. A campus policy establishes a decentralized compliance structure for ensuring that credit card processing contracts and purchases are properly initiated, that compliance questionnaires are completed, and that controls are appropriate to ensure compliance with the PCI DSS. Notably, CSULB has formally documented all credit card processing activities and has taken steps to determine compliance with PCI Data Standard version 3.2, which is not required to be implemented until June 2016.

SCOPE

We visited CSULB from September 21, 2015, through October 9, 2015. Our audit and evaluation included the audit tests we considered necessary in determining whether payment card processing controls are in place and operative. The audit focused on procedures in effect from January 1, 2014, through August 30, 2015.

Specifically, we reviewed and tested:

- Processes to identify all credit card-processing activities on the campus and establishment of plans to address the associated risks.
- Establishment of a campuswide PCI compliance program that includes completion of PCI compliance reports, validation of applicable system and network controls, and scanning.
- Processes to ensure that the control framework for payment card processing is complete, and that controls are operating effectively.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

Our testing and methodology was designed to provide a managerial-level review of payment card processing activities, which included detailed testing on a limited number of payment card processing controls. Our review was not intended to formally assess or validate campus compliance with PCI DSS.

CRITERIA

Our audit was based upon standards as set forth in CSU Board of Trustee policies; Office of the Chancellor policies, letters, and directives; campus policies and procedures; and other sound administrative practices. This audit was conducted in conformance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

This review emphasized, but was not limited to, compliance with:

- ICSUAM §8000, *Information Security*
- PCI DSS 3.1, *Requirements and Security Assessment Procedures,* dated April 2015

AUDIT TEAM

Senior Director: Mike Caldera
Audit Manager: Greg Dove