STATE OF ILLINOIS
OFFICE OF THE
AUDITOR GENERAL
Frank J. Mautino, Auditor General

SUMMARY REPORT DIGEST

GOVERNORS STATE UNIVERSITY

State Compliance Examination
For the Year Ended June 30, 2023

Release Date: May 7, 2024

FINDINGS THIS AUDIT: 12			
	New	Repeat	Total
Category 1:	**0**	**0**	**0**
Category 2:	**3**	**8**	**11**
Category 3:	**1**	**0**	**1**
TOTAL	**4**	**8**	**12**
FINDINGS LAST AUDIT: 9			

AGING SCHEDULE OF REPEATED FINDINGS			
Repeated Since	**Category 1**	**Category 2**	**Category 3**
2021		**23-02, 23-10 23-11, 23-12**	
2020		**23-06**	
2019		**23-08**	
2016		**23-09**	
2005		**23-07**	

INTRODUCTION

This digest covers the Governors State University (University) Compliance Examination for the year ended June 30, 2023. Separate digests covering the University's Financial Audit and Single Audit as of and for the year ended June 30, 2023 were previously released on March 28, 2024. In total, this report contains 12 findings, 5 of which were reported in the Financial Audit and Single Audit collectively.

SYNOPSIS

- **(23-06)** The University did not have adequate internal control over reporting its census data.
- **(23-10)** The University did not have adequate controls over its service providers.
- **(23-12)** The University has not completed all requirements to demonstrate full compliance with Payment Card Industry Data Security Standards.

Category 1: Findings that are **material weaknesses** in internal control and/or a **qualification** on compliance with State laws and regulations (material noncompliance).

Category 2: Findings that are **significant deficiencies** in internal control and **noncompliance** with State laws and regulations.

Category 3: Findings that have **no internal control issues but are in noncompliance** with State laws and regulations.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

INADEQUATE INTERNAL CONTROLS OVER CENSUS DATA

The University did not have adequate internal control over reporting its census data to provide assurance census data submitted to its pension and other postemployment benefits (OPEB) plans was complete and accurate.

7 instances of member information being reported to SURS after the close of the fiscal year

During our cut-off testing of data transmitted by the University to SURS, we noted 6 instances of an inactive employee becoming active and 1 instance of an active employee becoming inactive were reported to SURS after the close of the fiscal year in which the event occurred. Two of these instances have been previously reported, however still impacted the June 30, 2021 census data. SURS determined the total potential impact of these errors was the instructors' service credit was off by a combined 1 year. (Finding 6, Pages 19-20)

We recommended the University continue to focus on the incremental changes to the census data file from the prior actuarial valuation, provided no risks are identified that incomplete or inaccurate reporting of census data may have occurred during prior periods. Any errors identified during this process should be promptly corrected by either the University or SURS, with the impact of these errors communicated to both SURS' actuary and CMS' actuary. Further, we recommended the University ensure all events occurring within a census data accumulation year are timely reported to SURS so these events can be incorporated into the census data provided to SURS' actuary and CMS' actuary

University agreed with the auditors

University officials agreed with the finding and stated the University has been working to address the issues identified.

INADEQUATE CONTROLS AROUND SERVICE PROVIDERS

The University did not have adequate controls over its service providers.

In Fiscal Year 2023, the University identified 72 service providers. The University maintains numerous cloud-based solutions with various service providers. These service providers maintain the hardware, software and the data for various applications regarding many sectors, such as campus news and events, student orientation, employment, photographs, student organizations, visitor tracking, course evaluations, and emergency notifications.

We requested the University provide a population of service providers utilized during the examination period to determine

if the University had reviewed the internal controls over its service providers. In response to our request, the University provided a population; however, the population contained inaccuracies related to identifying which vendors qualify as service providers. Due to these conditions, we were unable to conclude the University's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accounts (AT-C 205.36). Despite this limitation, we proceeded to conduct a detailed testing over seven service providers and noted the University had not:

For 100% of the service providers tested, the University did not have documented procedures for monitoring of service providers or timely reviewed SOC reports

- Developed formal, documented policies and procedures to ensure performance measures are monitored to comply with contractual terms for seven (100%) service providers.
- Timely reviewed System and Organization Control (SOC) reports for seven (100%) service providers.
- Monitored and documented the operation of the Complementary User Entity Controls (CUECs) relevant to the University's operations for five (71%) service providers.

For 86% of the service providers tested, the University did not obtain and review SOC reports or perform alternate procedures for subservice providers

- Obtained and reviewed SOC reports for the subservice providers or performed alternative procedures to determine the impact on the University's internal control environment for six (86%) service providers.
- Conducted an analysis to determine the impact of noted deviations within SOC reports for one (14%) service provider.

The University is responsible for the design, implementation, and maintenance of internal controls related to information systems and operations to ensure resources and data are adequately protected from unauthorized or accidental disclosure, modifications, or destruction. This responsibility is not limited due to the process being outsourced. (Finding 10, Pages 28-29)

We recommended the University:

- Establish policies and procedures to ensure performance measures are monitored to comply with contractual terms and service level agreements.
- Timely review SOC reports of the service providers.
- Monitor and document the operation of the CUECs noted in the SOC reports that are relevant to the University's operations.
- Obtain and review the SOC reports of subservice providers or perform alternative procedures to determine the impact on the internal control environment of the University.
- Conduct an analysis to determine the impact of noted deviations on the SOC reports to the University's internal control environment.

University agreed with auditors

University officials agreed with the finding and stated they have assigned additional resources to service providers' reviews.

WEAKNESSES WITH PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

The University had not completed all requirements to demonstrate full compliance with the Payment Card Industry Data Security Standards (PCI DSS).

In Fiscal Year 2023, the University accepted approximately 19,654 credit card transactions estimated at $15.5 million.

University had not assessed PCI DSS at all locations or validated all elements of its cardholder data environment

Upon review of the University's efforts to ensure compliance with PCI DSS, we noted the University had not:

- Established formal policies over processing of PCI transactions;
- Completed formal assessments of each location (14 of 19 merchants) accepting credit card payments, including the appropriate Self-Assessment Questionnaire (SAQ) and certifying compliance;
- Validated merchants for all elements of its cardholder data environment verifying PCIDSS compliance; and
- Ensured all employees involved in the processing of cardholder data received annual security training. (Finding 12, Pages 32-33)

We recommended the University:

- Establish policies dedicated to the processing of PCI transactions. Such policies would establish the framework for procedures to ensure PCI DSS compliance.
- At least annually, assess each location accepting credit card payments and match the method of acceptance to the appropriate SAQ and complete the appropriate SAQ(s) for its environment and maintain documentation.
- Validate merchants for all elements of its cardholder data environment verifying PCI DSS compliance.
- Provide annual security training to employees involved in the processing of cardholder data.

University agreed with auditors

University officials agreed with the finding and stated they have been working toward full compliance with PCI DSS.

OTHER FINDINGS

The remaining findings are reportedly being given attention by the University. We will review the University's progress towards the implementation of our recommendations in our next engagement.

AUDITOR'S OPINIONS

The financial audit was previously released. Our auditors stated the financial statements of the University as of and for the year ended June 30, 2023 are fairly stated in all material respects.

The single audit was previously released. Our auditors also conducted a Single Audit of the University as required by the Uniform Guidance and stated the University complied, in all material respects, with the types of compliance requirements that could have a direct and material effect on the University's major federal programs for the year ended June 30, 2023.

ACCOUNTANT'S OPINION

The accountants conducted a State compliance examination of the University for the year ended June 30, 2023, as required by the Illinois State Auditing Act. The accountants stated the University complied, in all material respects, with the requirements described in the report.

This State compliance examination was conducted by Adelfia LLC.

SIGNED ORIGINAL ON FILE

JANE CLARK
Division Director

This report is transmitted in accordance with Section 3-14 of the Illinois State Auditing Act.

SIGNED ORIGINAL ON FILE

FRANK J. MAUTINO
Auditor General

FJM:JGR