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, 2024

Release Date: May 22, 2025

FINDINGS THIS AUDIT: 17

	New	Repeat	Total
Category 1:	0	0	0
Category 2:	4	10	14
Category 3:	3	0	3
TOTAL	7	10	17

FINDINGS LAST AUDIT: 12

AGING SCHEDULE OF REPEATED FINDINGS

Repeated Since	Category 1	Category 2	Category 3
2023		24-01, 24-03	
2021		24-02, 24-15, 24-16, 24-17	
2020		24-08	
2019		24-13	
2016		24-14	
2005		24-12	

INTRODUCTION

This digest covers the Governors State University (University) Compliance Examination for the year ended June 30, 2024. Separate digests covering the University's Financial Audit and Single Audit as of and for the year ended June 30, 2024 were previously released on March 27, 2025. In total, this report contains 17 findings, 7 of which were reported in the Financial Audit and Single Audit collectively.

SYNOPSIS

- **(24-08)** The University did not have adequate internal control over reporting its census data.
- **(24-11)** The University had deficiencies within its internal audit activities.
- **(24-15)** The University did not have adequate controls around its service providers.
- **(24-17)** 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 and did not have a reconciliation process to provide assurance census data submitted to its pension and other postemployment benefits (OPEB) plans was complete and accurate.

4 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 3 instances of an inactive employee becoming active and 1 instance of an active employee becoming active were reported to SURS after the close of the fiscal year in which the event occurred. These instances have been previously reported, however still impacted the June 30, 2022 census data. SURS determined the total potential impact of these errors was the instructors' service credit was off by a combined 6.75 years. (Finding 8, Pages 22-23) **This finding has been reported since 2020.**

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 already established procedures to correct the issues.

INTERNAL AUDIT DEFICIENCIES

The University had deficiencies within its internal audit activities.

During our testing, we noted the following:

3 internal audit report were not provided to auditors

- Three of 4 (75%) audit reports had not been provided to the auditors. Additionally, the internal audit workpapers for two sample audit reports remain outstanding. The University's Chief Internal Auditor (CIA) reported four complete audits in the annual report dated September 30, 2024 to the University's President.

Failure to conduct an external assessment during the examination period

- The University's internal audit function failed to conduct a new external assessment during the examination period as required. The last external assessment was conducted in July 2018. Additionally, the annual audit report dated September 30, 2024, incorrectly stated that internal audit engagements were conducted in accordance with International Standards for the Professional Practice of Internal Auditing (IPPIA). (Finding 11, Pages 26-27)

We recommended the University improve its procedures to ensure timely finalization of its audit documentation. We further recommended the University to conduct a periodic external assessment of the internal audit function, in compliance with the IPPIA standards.

University agreed with the auditors

University officials agreed with the finding and stated the University will work toward full compliance.

INADEQUATE CONTROLS AROUND SERVICE PROVIDERS

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

In Fiscal Year 2024, the University identified 86 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.

During testing of 21 service providers, we noted the University had not:

For 100% of the service providers tested, the University did not have documented procedures for monitoring of service providers

- Developed formal, documented policies and procedures to ensure performance measures are monitored to comply with contractual terms for the service providers tested (100%).
- Performed a review of the System and Organization Control (SOC) reports for two (10%) service providers.
- Timely reviewed the System and Organization Control (SOC) reports for 16 (76%) service providers, with reviews conducted between 100 to 863 days after report issuance.

For 57% of the service providers tested, the University did not review CUECs

- Assessed and documented the operation of Complementary User Entity Controls (CUECs) relevant to the University's operations for 12 (57%) service 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 19 (90%) service providers.
- Conducted an analysis to determine the impact of modified opinions and control deviations on 2 (50%) of 4 SOC reports.

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 15, Pages 35-37) **This finding has been reported since 2021.**

We recommended the University:
- Establish policies and procedures to ensure performance measures are monitored to comply with contractual terms and service level agreements.
- Obtain and review SOC reports of the service providers.
- Perform timely review of 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 will continue efforts toward compliance with the recommendations.

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 2024, the University accepted approximately 18,815 credit card transactions estimated at $15.3 million.

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

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

- Completed formal assessments of each merchant 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 PCI DSS compliance;
- Ensured all employees involved in the processing of cardholder data received annual security training; and
- Maintained an agreement with each service provider which requires the service provider to ensure validated PCI compliance for the services/solutions being provided. (Finding 17, Pages 40-41) **This finding has been reported since 2021.**

University did not maintain agreements with service providers

We recommended the University:

- 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.
- Maintain an agreement with each service provider which requires the service provider to ensure validated PCI compliance for the services/solutions being provided.

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 State compliance examination.

AUDITOR'S OPINIONS

The auditors stated the financial statements of the University as of and for the year ended June 30, 2024, are fairly stated in all material respects.

The auditors also conducted a Single Audit of the University as required by the Uniform Guidance. The auditors 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, 2024.

ACCOUNTANT'S OPINION

The accountants conducted a State compliance examination of the University for the year ended June 30, 2024, as required by

the Illinois State Auditing Act. The accountants stated the University complied, in all material respects, with the requirements describe in the report.

This State compliance examination was conducted by Adelfia LLC.

SIGNED ORIGINAL ON FILE

COURTNEY DZIERWA
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