




STATE OF ILLINOIS ILLINOIS STATE UNIVERSITY

Report Required under Government Auditing Standards
For the Year Ended June 30, 2025

Performed as Special Assistant Auditors
for the Auditor General, State of Illinois



State of Illinois
Illinois State University
Contents
For the Year Ended June 30, 2025

Table of Contents

University Officials	1
-----------------------------------	----------

Government Auditing Standards Report

Summary	2
---------------	---

Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with Government Auditing Standards	3
--	---

Schedule of Findings

Current Findings.....	5
-----------------------	---

Prior Findings Not Repeated.....	10
----------------------------------	----

Other Reports Issued Under a Separate Cover

The Illinois State University's Federal Single Audit and State Compliance Examination for the year ended June 30, 2025, will be issued under separate covers. Additionally, the University's financial statements as of and for the year ended June 30, 2025, have been issued under a separate cover.

**State of Illinois
Illinois State University
Financial Audit
For the Year Ended June 30, 2025**

University Officials

President	Dr. Aondover Tarhule
Vice President for Finance and Planning (01/06/25 – present)	Dr. Glen Nelson
Vice President for Finance and Planning (01/01/25-01/05/25)	Vacant
Interim Vice President for Finance and Planning (07/01/24 – 12/31/24)	Mr. Dan Petree
Vice President for Academic Affairs and Provost	Dr. Ani Yazedjian
Vice President for Student Affairs	Dr. Levester Johnson
Vice President for University Advancement	Mr. Pat Vickerman
Comptroller (12/02/24 – present)	Mr. Carlos Garcia
Comptroller (07/01/24 – 12/31/24)	Mr. Doug Schnittker
Legal Counsel	Ms. Jeannie Barrett
Director – Internal Audit	Mr. Robert Blemler

Officers of the Board of Trustees

Chair of the Board	Dr. Kathryn Bohn
Secretary of the Board	Dr. Robert Navarro

Members of the Board of Trustees

Member	Dr. Kathryn Bohn
Member	Dr. Robert Navarro
Member (05/02/25 – present)	Ms. Julie Hoeniges
Member (02/22/25 – 05/01/25)	Vacant
Member (07/01/24 – 02/21/25)	Ms. Julie Annette Jones
Member (08/01/25 – present)	Mr. Kris Lutt
Member (07/26/25 – 07/31/25)	Vacant
Member (07/01/24 – 07/25/25)	Mr. Scott Jenkins
Member	Dr. Lia Merminga
Member (06/06/2025 – present)	Mr. Doug Peterson
Member	Mr. Darren Tillis
Student Member	Mr. Ryan Russell

Office Location

The University's primary administrative offices are located at:

Hovey Hall
Campus Box 1100
Normal, Illinois 61790-1100

**State of Illinois
Illinois State University
Schedule of Findings
For the Year Ended June 30, 2025**

Summary

The audit of the financial statement of the Illinois State University (University) was performed by Forvis Mazars, LLP in accordance with *Government Auditing Standards*. This report is an integral part of that audit.

Based on their audit, the auditors expressed an unmodified opinion on the University's basic financial statements, issued under a separate cover.

Summary of Findings

The auditors identified three matters involving the University's internal control over financial reporting that they considered to be material weaknesses.

Item No.	Page	Last/First Reported	Description	Finding Type
Findings (<i>Government Auditing Standards</i>)				
2025-001	5	2025/2018	Information Security Weaknesses	Material Weakness
2025-002	7	2025/2023	Lack of Adequate Controls over the Review of Internal Controls over Service Providers	Material Weakness
2025-003	9	2025/2023	Weakness in Change Control	Material Weakness

Exit Conference

The findings and recommendations appearing in this report were discussed with University personnel at an exit conference on November 13, 2025. In attendance were:

Attending were:

Illinois State University

Dr. Glen Nelson	Vice President for Finance and Planning
Carlos Garcia	Comptroller
Erika Jones	Assistant Comptroller
Emily Duffield	Chief Accountant
Rob Blemler	Director – Internal Auditing and University Ethics Officer

Office of the Auditor General

Thomas Kizziah	Senior Audit Manager
Reddy Bommareddi	Senior Audit Manager

Forvis Mazars, LLP

Heather Powell	Partner
----------------	---------

The responses to the recommendations were provided by Ms. Erika Jones, Assistant Comptroller, in a correspondence dated November 6, 2025.

**Report on Internal Control over Financial Reporting and
on Compliance and Other Matters Based on an Audit of
Financial Statements Performed in Accordance With
*Government Auditing Standards***

Independent Auditor's Report

Honorable Frank J. Mautino
Auditor General
State of Illinois

and

The Board of Trustees
Illinois State University

As Special Assistant Auditors for the Auditor General, we have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States (*Government Auditing Standards*), the financial statements of the business-type activities, fiduciary activities, and the discretely presented component unit of the Illinois State University (University), collectively a component unit of the State of Illinois, as of and for the year ended June 30, 2025, and the related notes to the financial statements, which collectively comprise the University's basic financial statements, and have issued our report thereon dated December 3, 2025. Our report includes a reference to other auditors who audited the financial statement of the Illinois State University Foundation, as described in our report on the University's financial statements. The report does not include the results of the other audits' testing of internal control over financial reporting or compliance and other matters that are reported on separately by those auditors.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the University's financial statements will not be prevented or detected and corrected on a timely basis. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and, therefore, material weaknesses or significant deficiencies may exist that were not identified. We identified certain deficiencies in internal control, described in the accompanying schedule of findings and responses as items 2025-001, 2025-002, and 2025-003 that we consider to be material weaknesses.

Report on Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

University's Response to Findings

Government Auditing Standards requires the auditor to perform limited procedures on the University's response to the findings identified in our audit and described in the accompanying schedule of findings and responses. The University's response was not subjected to the other auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on the response.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the University's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the University's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

SIGNED ORIGINAL ON FILE

Decatur, Illinois
December 3, 2025

Current Findings – Government Auditing Standards

Finding 2025-001 Information Security Weaknesses

The Illinois State University (University) had multiple computer security weaknesses.

The University relies on its computing environment for maintaining several critical, sensitive, and/or confidential systems used to meet its mission.

During testing of University information technology controls, we noted the University:

- Had not fully developed access provisioning policies documenting the internal controls for all environments and applications.
- Had not fully developed a policy documenting requirements for an annual review of users' access.
- Had not fully developed a policy documenting the review of security violation reports to ensure remediation is timely conducted.

In order to determine if proper security controls had been implemented across the University's environment, we requested a population of servers. Although the University provided a population, documentation demonstrating its completeness and accuracy was not provided. Due to these conditions, we were unable to conclude the Office's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AU-C § 330, AT-C § 205). Even given the population limitations, we tested the population of servers, noting the University could not provide documentation demonstrating the antivirus and operating system were running the vendors' latest versions.

In addition, our testing noted the University had not ensured all security operations were properly configured.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Access Control and Configuration Management sections require entities to maintain proper internal controls over access and security of their environment, applications and data.

Also, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

University officials indicated the IT functions and resources are highly distributed across the institution which require considerably more time to change and improve. University officials also indicated IT is limited in capacity to fully organize the remediation efforts within the portfolio of work efforts required of IT across the institution.

Inadequate controls over changes to the University's environment, applications and data could lead to unauthorized access, unauthorized changes and security risks to its environments, applications and related data. Also, due to the severity of the weaknesses noted, we were unable to rely upon the general IT controls over the environments and applications. (Finding Code No. 2025-001, 2024-001, 2023-001, 2022-002, 2021-002, 2020-003, 2019-001, 2018-002)

Finding 2025-001 Information Security Weaknesses (continued)

Recommendation

We recommend the University implement adequate security, including approving the updated policies and procedures to (1) reflect the University's current environment and (2) address future changes in processes and new systems.

Additionally, we recommend the University strengthen its controls to maintain a complete and accurate population of servers, update their servers with the vendors' latest versions of antivirus and operating systems, and ensure all security operations are properly configured.

University Response

The University agrees with the observations reported in this finding.

To directly address this root cause, the University initiated an organizational realignment. Effective June 11, 2025, the Chief Information Security Officer (CISO) reporting line was moved to the Vice President of Finance and Planning to elevate the priority of institutional governance, risk, and compliance. Furthermore, on July 25, 2025, the Board of Trustees formally designated the CISO as the "Qualified Individual" (QI) for the University's information security program.

These foundational changes provide the necessary authority and prioritization to complete the corrective action plan. The University expects the results of this plan to be evident within the FY26 audit review period. Specific progress at the time of response includes:

- **Policy Development:** The policies identified in the finding (including access provisioning, annual user access reviews, and security violation reporting) are in the drafting and socialization phase. With the CISO's new authority, these are targeted for formal approval within Fiscal Year 2026 (FY26).
- **Asset & Configuration Management:** The University has matured and validated its automated asset inventory process using our advanced Extended Detection and Response (XDR) solution. This addresses the auditors' concerns regarding a complete server population and provides documented data on security configurations.
- **Security Standards:** To address configuration, patching, and operating system weaknesses, the University has developed and implemented new standards for patch management, vulnerability management, local administrator restrictions, and user account management. Additional standards for remote access, privileged access, and device threat protection are also in development.

Finding 2025-002 Lack of Adequate Controls over the Review of Internal Controls over Service Providers

The Illinois State University (University) did not implement adequate internal controls over its service providers.

We requested the University provide a population of their service providers utilized in order to determine if the University had reviewed the internal controls of its service providers. However, the University was not able to provide such a population. Additionally, we noted the University had not fully developed policies and procedures to ensure their due diligence and monitoring of their service providers. Furthermore, the University did not obtain System and Organization Control (SOC) reports to ensure the internal controls at the service providers had been implemented and were operating effectively. Finally, the University had not conducted a review of the Complementary User Entity Controls (CUEC) and the University's related controls.

Due to these conditions, we were unable to determine if the internal controls of the service providers were adequate, and we were required to perform alternative procedures.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Maintenance and System and Service Acquisition sections, requires entities outsourcing their information technology environment or operations to obtain assurance over the entities' internal controls related to the services provided. Such assurance may be obtained via System and Organization Control reports or independent reviews.

Also, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

University leadership did not have sufficient time to fully develop and implement the current strategy for holistic service provider management before the end of the fiscal year. As a result, the various functions related to service provider oversight remain distributed across multiple departments. As of June 30, 2025, the university continued to develop a comprehensive strategy and framework to analyze and manage its service provider population. A draft policy was created to establish this framework and define the necessary roles and responsibilities for effective management; however, this process was not completed prior to June 30, 2025.

Without having obtained and reviewed SOC reports or another form of independent internal control review, the University does not have assurance the service providers' internal controls are adequate and operating effectively. (Finding Code No. 2025-002, 2024-002, 2023-002)

Recommendation

We recommend the University implement controls to maintain a list of all of their service providers and determine and document if a review of the service providers' internal controls were performed, if required.

Additionally, we recommend the University:

- Obtain SOC reports or perform independent reviews of internal controls for all service providers.
- Monitor and document the operation of the CUECs relevant to the University's operations.
- Either obtain and review SOC reports for subservice organizations or perform alternative procedures to satisfy itself that the existence of the subservice organization would not impact its internal control environment.

Finding 2025-002 Lack of Adequate Controls over the Review of Internal Controls over Service Providers (continued)

- Document its review of the SOC reports and review all significant issues with subservice organizations to ascertain if a corrective action plan exists and when it will be implemented, any impacts to the University, and any compensating controls.

University Response

The University acknowledges and agrees with the auditor's findings and recommendations to implement controls to maintain a list of all its service providers. We agree that the absence of a robust framework for service provider oversight can expose the organization to potential risks, including operational inefficiencies, compliance issues, and security vulnerabilities.

The University remains committed to addressing this gap and continues its efforts to:

- Complete and fully implement the policy (currently in draft version) that provides a framework for managing the lifecycle of vendor relationships and provide context for University's procedures that outline specific systems and guidelines for vendor management.
- Establish controls for vendor selection and risk evaluation process.
- Strengthen ongoing monitoring and performance reviews of service providers including obtaining, documenting, and reviewing SOC reports to identify risk and action plans to minimize risks and address any control deficiencies.
- Ensure regular audits and assessments of service providers to mitigate risks and ensure alignment with organizational objectives and regulatory requirements.

Finding 2025-003 Weaknesses in Change Control

The Illinois State University (University) did not maintain adequate internal controls over changes to its environment, applications and data.

The University had not fully developed a change management policy documenting the internal controls over changes to its environment, applications and data. In addition, the University had not fully implemented a formal Change Management Board.

Further, the approval for changes, including emergency changes, prior to being implemented into production was not maintained.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Configuration Management section, require entities to maintain proper internal controls over the changes to the environment, applications and data.

Also, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

University officials indicated that the lack of a unifying and fully approved policy continues to be the cause of the noted gaps. A draft policy was developed but was not fully reviewed and implemented prior to June 30, 2025.

Inadequate controls over changes to the University's environment, applications and data could lead to unauthorized access, unauthorized changes and security risks to its environments, applications and related data. Also, due to the severity of the weaknesses noted, we were unable to rely upon the general IT control over the environments and applications. (Finding Code No. 2025-003, 2024-003, 2023-003)

Recommendation

We recommend the University implement adequate policies and procedures over changes to the University's environment, applications and data. We also recommend the University maintain documentation that changes are properly approved prior to implementation.

University Response

The University acknowledges and agrees with the auditor's findings and recommendations for a university-wide policy governing changes in systems regardless of system ownership. While there were documented procedures and controls as well as a governing body that meets weekly to review and approve changes in systems owned by central IT, there is a need for a formal policy and to ensure consistency across campus. A draft policy was finalized prior to June 30th, 2025, and is currently being reviewed for adoption in fiscal year 2026.

Procedures have been modified to ensure that all emergency changes are finalized and recorded in the Information Technology Service Management software.

**State of Illinois
Illinois State University
Schedule of Findings
For the Year Ended June 30, 2025**

Prior Findings Not Repeated

None