LEGISLATIVE AUDIT COMMISSION

Review of
Southern Illinois University
Year Ended June 30, 2024

620 Stratton Office Building
Springfield, Illinois 62706
217/782-7097

REVIEW: #4606
SOUTHERN ILLINOIS UNVERISTY
YEAR ENDED JUNE 30, 2024

FINDINGS/RECOMMENDATIONS – 14

IMPLEMENTED/PARTIALLY IMPLEMENTED – 8
UNDER STUDY - 6

REPEATED RECOMMENDATIONS – 10

PRIOR AUDIT FINDINGS/RECOMMENDATIONS – 17

This review summarizes the auditors' report of Southern Illinois University for the year ended June 30, 2024, filed with the Legislative Audit Commission on September 30, 2025. The auditors conducted a compliance examination in accordance with state law and Government Auditing Standards.

Agency Narrative

Founded in 1869, the Southern Illinois University System includes nationally recognized public universities serving more than 24,500 students across two institutions: Southern Illinois University Carbondale (SIUC) and Southern Illinois University Edwardsville (SIUE). SIUC includes a School of Law in Carbondale and a School of Medicine in Springfield. SIUE includes a School of Pharmacy in Edwardsville, a School of Dental Medicine in Alton, the Southwestern Illinois Justice and Workforce Development Campus in Belleville and the East St. Louis Center. Employing more than 7,400 faculty and staff, the SIU System is a major economic driver for central and southern Illinois and offers a wide range of academic programs leading to associate, bachelor's, master's, specialist, doctoral and professional degrees including law, medicine, pharmacy and dental medicine.

Dr. Daniel Mahony has served as President since March 2020. Before coming to the SIU system, Dr. Mahony served as President of Winthrop University in Rock Hill, South Carolina from 2015 to 2020.

Appropriations and Expenditures

Appropriations ($ thousands)	FY23		FY24	
	Approp	Expend	Approp	Expend
GENERAL FUNDS				
Designated Purposes				
Daily Egyptian Newspaper	62.8	62.8	62.8	62.8
Institute of Rural Health	0.0	0.0	300.0	49.0

National Corn-to-Ethanol Research Center	1,000.0	1,000.0	1,000.0	1,000.0
Office of Community Engagement	0.0	0.0	266.6	172.7
Operational Expenses	201,065.6	201,065.6	215,140.2	215,140.2
Programming at Lindenwood Campus	3,500.0	2,867.9	3,500.0	3,454.5
Simmons Cancer Institute at SIU	1,076.8	1,076.8	1,130.6	1,130.6
TOTAL GENERAL FUNDS	**206,705.2**	**206,073.1**	**221,400.2**	**221,009.8**
OTHER STATE FUNDS				
Designated Purposes				
Pharmacy Practice Educ. & Train. Programs at Edwardsville	1,250.0	1,250.0	1,250.0	1,250.0
Grants				
Scholarship Grant Awards	17.0	17.0	17.0	17.0
TOTAL OTHER STATE FUNDS	**1,267.0**	**1,267.0**	**1,267.0**	**1,267.0**
TOTAL	**207,972.2**	**207,340.1**	**222,667.2**	**222,276.8**

Accountants' Findings and Recommendations

Condensed below are the 14 findings and recommendations included in the audit report. Of these, 10 are repeated from the previous audit. The following recommendations are classified on the basis of information provided by SIU of, via electronic mail received December 2, 2025.

1. **The auditors recommend the University ensure performance of appropriate reviews of invoice details to ensure the service period is being utilized to determine the period in which accounts payable and accrued liabilities and the related expenses are recorded in the financial statements. They also recommend the University review the service date entered into the system to ensure amounts are accrued in the proper fiscal year.**

   Additionally, they recommend the University input a control to timely review for payments on fixed assets to ensure expenses are being properly capitalized in the correct period.

FINDING: *Inadequate Internal Controls over Cutoff of Accounts Payable and Accrued Liabilities – New*

Southern Illinois University (University) did not have adequate internal controls over cutoff of accounts payable and accrued liabilities to ensure amounts owed are recorded in the proper period.

During testing performed within the financial statement audit, the auditors noted the following:

- The University recorded two invoices for $206,741 and $613,025, respectively, in accounts payable as of June 30, 2024. However, the services related to fiscal year 2025.

- The University recorded a duplicate invoice for $161,675 in accounts payable as of June 30, 2024.

- The University did not record an invoice for $48,163 in accounts payable as of June 30, 2024 although the goods were received in fiscal year 2024.

- The University accrued and expensed, rather than capitalized, two fixed assets for $263,770 during fiscal year 2024.

The University did not record adjustments to the financial statements for these misstatements.

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 that expenditures, resources, or funds applicable to operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial reports. Good internal control procedures require adequately trained personnel with the knowledge, skills and experience to prepare GAAP-based financial statements, management oversight and review of accounting policies and procedures, as well as an overall review of financial reporting for accuracy and compliance with GAAP.

Governmental Accounting Standards Board (GASB) Statement No. 62 – *Codification of Accounting and Financial Reporting Guidance Contained in Pre-November 30, 1989 FASB and AICPA Pronouncements* requires government-wide financial statements to be prepared using the economic resources measurement focus and the accrual basis of accounting. The accrual basis of accounting records revenues and expenses when they are earned or incurred, regardless of when the cash is actually received or paid. GASB 62, paragraph 34, also requires current liabilities to be used principally to designate obligations whose liquidation is reasonably expected to require the use of existing resources properly classifiable as current assets, or the creation of other current liabilities.

University officials indicated some errors were caused by improper input of the service date within the accounting system in instances where the service period did not match the invoice date and crossed fiscal reporting periods. Officials indicated the duplicate invoice was recorded due to a lack of review of accruals impacted by voided checks as of June 30, 2024. Officials also indicated fixed assets were not timely reviewed to determine if they should be capitalized as of June 30, 2024.

These deficiencies in the University's internal control over financial and fiscal operations poses a reasonable possibility that a misstatement of the University's financial statements will occur and not be prevented or detected and corrected on a timely basis. Accurate preparation of the University's financial information for GAAP and financial reporting

purposes is important due to the impact adjustments may have on the Statewide financial statements.

UNIVERSITY RESPONSE:
Agree. The University will ensure that appropriate reviews of invoice details are performed so that accurate service dates are entered into the accounting system in order to properly record accrued expenses. The results of the audit were reviewed with accounts payable staff, and additional training has been provided to underscore the importance of the accuracy of the service dates to ensure expenditures are properly recorded in either the prior or current fiscal year. Each year at fiscal year-end, the Accounts Payable supervisor will meet with staff to provide refresher training on this issue. Accounts Payable staff have been encouraged to seek guidance and further review of any invoices in which the service dates are not clearly discernable.

Also, the University will implement the following control regarding payments on fixed assets to ensure expense capitalization in the proper period. Any invoices entered and corresponding payments made in July that are accruable due to receipt of equipment prior to July 1st will be shared with the respective Property Control staff for review and inclusion as capitalized assets as needed. The results of this audit were shared with Property Control staff. Recording an expense accrual in the prior year as well as capitalizing the equipment into the prior year fixed assets period will ensure that the applicable expense and capitalization will occur in the same fiscal year.

UPDATED RESPONSE:
Implemented.
No change**.** Director of Accounting Services (Carbondale) and Director of Administrative Accounting (Edwardsville).

2. **The auditors recommend the University strengthen its process and controls to identify and document all service providers utilized across campuses and determine and document if a review of controls is required. Where appropriate, they recommend the University:**

    - **Obtain and retain SOC reports (or perform independent reviews) and bridge letters, and document the assessment of internal controls associated with outsourced systems at least annually.**

    - **Monitor and adequately document the operation of the CUECs related to the University's operations.**

    - **Obtain and review contracts with service providers to ensure applicable requirements over the independent review of internal controls are included.**

- **Implement a formal process to monitor and track service-level agreements for service providers to ensure all provisions are met and meet contract requirements.**

FINDING: *Lack of Adequate Controls over the Review of Internal Controls for Service Providers – This finding has been repeated since 2018.*

Southern Illinois University (University) lacked adequate controls over the review of its service providers.

The University utilized over 100 service providers for various services including, but not limited to banking, investment, and business services; debt financing; information technology hosting services; and software as a service.

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.

There is no formal University-wide requirement, defined in policy or procedure, to require an annual review of third-party service provider internal controls. As there was no University-wide requirement to obtain and review service organization control (SOC) reports for third-party service providers and no centralized oversight of third-party service providers, the auditors were unable to conclude the University's population records of third-party service providers were complete, accurate, and reliable under the Attestation Standards promulgated by the American Institute of Certified Public Accountants (AICPA) (AT-C 205.36).

Even given these population limitations, they selected a sample of service providers at each SIU campus from the listings provided and noted the following:

- Carbondale
  - For 6 of the 23 (26%) samples tested, the University did not obtain contracts that documented security, integrity, availability, confidentiality, and privacy controls over the University's data.
  - For 7 of 23 (30%) service providers tested, the University did not provide the SOC report and bridge letter utilized by the University to complete the SOC report review checklist for the third-party service provider.
  - For 9 of the 23 (39%) service providers tested, the University did not map existing University controls to complementary user entity controls.
- Edwardsville
  - For 1 of the 10 (10%) service providers tested, contracts were not provided for testing.
  - For 2 of the 10 (20%) service providers tested, the University did not obtain contracts that documented roles and responsibilities related to security, integrity, availability, confidentiality, and privacy controls over the University's data.

- For 2 of the 10 (20%) service providers tested, the University did not map existing University controls to complementary user entity controls.

- School Of Medicine
  - For 3 of 3 (100%) service providers tested, contracts and SOC reports were not provided for testing.

Additionally, across all university campuses, service-level agreements were not addressed within service provider contracts and were not tracked once the services had been agreed upon.

Weaknesses in the review of internal controls for service providers was first noted during the compliance examination for the year ended June 30, 2018. As such, the University has been unsuccessful in implementing sufficient corrective action to remedy all weaknesses noted.

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), System and Service Acquisition sections, requires entities outsourcing their IT environment or operations to obtain assurance over the entities internal controls related to the services provided. Additionally, the *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Special Publication 800-171, Third Revision) published by the National Institute of Standards and Technology (NIST), External System Services section, further supports monitoring of external providers for agency security compliance. Such assurance may be obtained via System and Organization Control reports or independent reviews.

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 that revenues, expenditures, and transfers of assets, resources, or funds applicable to operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the State's resources.

University management indicated the conditions noted were due to the complexities of implementing, coordinating, and executing a university wide program that requires buy in and participation from multiple stakeholders and departments.

The lack of a complete population of third-party service providers and the lack of a consistent process executed by the university departments to evaluate the third-party service providers impedes the process to identify and assess controls at service providers, which may impact integrity, availability, confidentiality, and security of university computer systems and data. Without having obtained and fully reviewed all SOC reports or another form of independent internal control review, the University does not have assurance that the service providers' internal controls are adequate.

UNIVERSITY RESPONSE:

Partially Agree. Implementation continues. SIU continues to refine and strengthen its processes. The current operational procedure was originally developed by the Software as a Service committee, which served as a foundational group to establish the third-party risk assessment framework. However, that committee is no longer active in an operational capacity; its role has since been replaced by a formalized process. Under this procedure, all third-party contracts must undergo an annual review prior to payment disbursement, including those with multi-year terms.

While the University does not require third-party vendors to provide SOC reports specifically, it does require formal attestation of the vendor's information security posture when deemed necessary through the review process. This attestation, preferably verified by an independent third party, such as via a SOC audit, helps clarify potential risks to the University and establishes accountability in the event of an incident or breach.

SOC reports contain highly sensitive data that could compromise the vendor's security perimeter. Currently, SOC reports and bridge letters are not provided because access typically requires individuals to agree to a non-disclosure agreement (NDA) with the service provider. These NDAs often restrict our ability to retain or share information beyond its intended purpose.

Additionally, storing such sensitive documentation could expose the University to liability if the reports are compromised. SOC reports are handled with the permission of the vendor as their property and can incur significant risk of liability if users retained them.

The University will engage in discussion with General Counsel and seek necessary guidance for a process that mitigates liability and aligns with compliance and audit requirements.

CUEC's are guidelines for completing the security configuration documented in the SOC report or attestation. They are not contractual obligations as they do not show in the contract. In most cases CUEC's can be unmappable because they are broad or vague, such as a control stating that the client must abide by the signed contract or Terms of Service.

Opportunities to further strengthen third-party risk assessment processes include evaluating the feasibility of implementing a dedicated third-party risk management system, subject to the availability of resources. Such a system would help streamline assessments, improve documentation, and enhance visibility into vendor-related risks across the institution.

ACCOUNTANT'S COMMENT:

As reported in the finding, the University did not require or perform annual reviews of internal controls for all third-party service providers. In addition, some SOC reports obtained by the University were not provided to the auditors.

SOC 1 reports are intended to be auditor to auditor communications. SOC 2 reports are intended for the information and use of the service organization, the user entity, and the user entities' auditors in accordance with attestation standards issued by the AICPA (AT-C 320.40). While we appreciate the University's caution when sharing such sensitive reports, these reports are integral to support the audit to obtain an understanding of the controls and operating deficiencies for third party service providers.

The Illinois State Auditing Act (30 ILCS 5/6-1) requires the disclosure of confidential information to the auditors as necessary for the audit and subjects such information to the same legal confidentiality and protective restrictions with the auditors as with the official authorized custodian.

Under the Attestation Standards promulgated by the AICPA, CUECs identified in a SOC report are controls which must be implemented by user entities in order to achieve the control objectives stated in management's description of the service organizations' system. All CUECs, despite the extent mapped to key controls, should be reviewed, evaluated, implemented, and acknowledged by the user entity. If there are CUECs identified, but the University does not ensure those controls are implemented, then the controls identified in the SOC report will not work effectively.

UPDATED RESPONSE:

Obtain and retain SOC reports (or perform independent reviews) and bridge letters, and document the assessment of internal controls associated with outsourced systems at least annually.

SIUC

• **Partially Implemented**: 75% complete. FY27 target completion. CISO. We obtain SOC reports and document the risk assessment and review of the SOC on an annual basis for all new contracts beginning in FY25, and as long-term contracts renew, they move into the same annual cycle.

• **Under Study**: Office of General Counsel + CISO. We do not currently retain SOC reports due to legal and contractual questions surrounding NDA necessary to obtain as well as the risk of retaining and securing confidential data belonging to our service providers. The stated 30 ILCS 5/6-1 statute in the findings does appear to provide the necessary avenue to be able to legally and contractually provide these documents to the Auditor General.

• *Monitor and adequately document the operation of the CUECs related to the University's operations.*

• SIUC **Partially Implemented**: 75% complete. FY27 target completion. CISO/IT GRC. We began documenting and mapping CUECs partway through FY25.

• *Obtain and review contracts with service providers to ensure applicable requirements over the independent review of internal controls are included.*

• SOM **Implemented**. IT/CISO. SOC2 review of providers.

SIUC
• **Under Study**: Director of Procurement, OGC, CISO/IT GRC. OIT will work in conjunction with procurement, OGC, and purchasing department to ensure the contract is included in review materials for the risk assessment.

- *Implement a formal process to monitor and track service-level agreements for service providers to ensure all provisions are met and meet contract requirements.*

  SIUC
  • **Under Study**: Director of Procurement, CISO/IT GRC. OIT will work with procurement and business units to develop a service level agreement monitoring plan. Campus business unit contracting the service.

  SIUE
  Under Study. Procurement Officers and Information Security Officers.

SIU continues to refine and strengthen its processes.

While the University does not require third-party vendors to provide SOC reports specifically, it does require formal attestation of the vendor's information security posture when deemed necessary through the review process. This attestation, preferably verified by an independent third party, such as via a SOC audit, helps clarify potential risks to the University and establishes accountability in the event of an incident or breach.

The University will engage in discussion with General Counsel and seek necessary guidance for a process that mitigates liability and aligns with compliance and audit requirements.

Opportunities to further strengthen third-party risk assessment processes include evaluating the feasibility of implementing a dedicated third-party risk management system, subject to the availability of resources. Such a system would help streamline assessments, improve documentation, and enhance visibility into vendor-related risks across the institution.

3. The auditors recommend the University strengthen internal controls over its cybersecurity programs and practices. Specifically, they recommend:

- **Each campus of the University enhances its risk assessment procedures to specifically include addressing the risks pertaining to confidential data controls, categorization of systems, and mitigating controls for legal risk.**
- **Each campus of the University identifies and evaluate data classification policies and monitoring controls, including identifying types of confidential data, systems, data owners, and evaluating the effectiveness of data controls and updating policies as needed.**

- **SIUC and SIUE implement privacy training for staff who handle Social Security Numbers (SSNs).**
- **SIUC and SIUE implement a process for regular reviews of policies and procedures, including a documented revision date and approval date.**
- **SIUE implement a campus wide acknowledgement process for policies and procedures.**
- **SIUC implement a Business Impact Analysis to identify confidential and personal information susceptible to attacks.**

FINDING: *Weakness in Cybersecurity Programs and Practices – This has been repeated since 2020.*

Southern Illinois University (University) had not fully implemented adequate internal controls related to cybersecurity programs and practices and control of confidential information.

The University carries out its mission with Information Technology, including various applications, which contain confidential or personal information such as names, addresses, social security numbers and health information of its students.

The Illinois State Auditing Act (30 ILCS 5/3-2.4) requires the Auditor General to review State agencies and their cybersecurity programs and practices. During their examination of the University's cybersecurity program, practices, and control of confidential information, the auditors noted:

Carbondale:

- SIUC had not defined or implemented a Business Impact Analysis process to identify confidential and personal information susceptible to attacks.
- SIUC had not addressed risks pertaining to controls over confidential data, or the categorization of systems. Data protection controls had not been outlined by data classification and there were no controls or mitigation plans documented to address legal risks identified during the Enterprise Risk Assessment.
- The Critical Controls Assessment did not include the inherent and control risks associated with SIUC data and the environment. The assessment should further identify the types of confidential data and systems, their associated risks, and categorize them accordingly.
- The Data Management/Safe Handling of Sensitive Information process, which outlines controls over data protection, had not been implemented.
- The Data Classification policy did not follow the requirements of the Identity Protection Act (5 ILCS 179), to reference this law. Additionally, the campus had no policy requiring staff who handle Social Security Numbers (SSNs) to be trained on SSN safe handling, to retain SSNs in a format that is easily redactable, or to provide a statement of purpose for social security number use upon request.
- Retention Schedules posted on the SIUC Records Management website did not include a documented revision date or approval date.

Edwardsville:

- SIUE had not implemented a campus-wide acknowledgement process for policies and procedures. Further, procedures at SIUE did not have a defined review schedule and did not appear to provide direct guidance for staff on how to report an incident.
- The University had not fully implemented a process to track and monitor confidential or sensitive data, and personally identifiable information at the University. Further, there were no controls or mitigation plans documented to address legal risks identified during the Enterprise Risk Assessment.
- The University did not provide evidence showing privacy training was implemented. While information technology (IT) staff received cybersecurity and operator training, privacy training was not enforced for staff who handle social security numbers.

School of Medicine:

- The Disaster Recovery plan did not include recovery scripts that outline step-by-step processes to recover systems.
- There were no specific controls implemented to track and monitor sensitive, confidential, or protected data or to, at a minimum, assess the classification level of data and monitor the systems and controls storing/protecting this data. Further, there were no controls or mitigation plans documented to address legal risks identified during the Enterprise Risk Assessment.

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.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) and the *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Special Publication 800-171, Third Revision) published by the National Institute of Standards and Technology (NIST), require entities to consider risk management practices, threat environments, legal and regulatory requirements, mission objectives and constraints in order to ensure the security of their applications, data, and continued business mission.

University management indicated weaknesses in cybersecurity programs and practices were due to limited resources and additional time needed to implement corrective action.

Failure to implement adequate security controls over the environment and devices exposes the University to increased danger of unauthorized access and the loss or corruption of critical and confidential data

UNIVERSITY RESPONSE:

Partially Agree. Implementation continues. The University has partially implemented adequate internal controls related to cybersecurity programs and practices and control of confidential information. The University continues to make consistent progress in strengthening its annual risk assessment process. This is particularly noteworthy given the continued decentralized nature of IT operations across certain campus units. Further enhancements are necessary, and the University remains committed to advancing these efforts throughout the upcoming fiscal year (FY26). A University Enterprise Risk Committee was established to develop an enterprise-wide risk management program that will identify, monitor, and categorize business risk.

Implementation procedures are not yet fully realized across all areas for established data protection policies and standards. Prioritization of the development and adoption of these procedures is in place to ensure consistent and effective application of our data protection framework.

Guidance on the handling of Personally Identifiable Information (PII)—including Social Security Numbers and student data—are a part of the mandatory annual SIUC cybersecurity training required for all employees. We believe this satisfies the core requirement for awareness and safe handling of sensitive data.

However, we will continue to assess and refine the training content to ensure it remains effective, relevant, and aligned with evolving compliance expectations.

While we acknowledge that procedural implementation in this area requires further development, SIUC maintains a regular, annual review of all IT policies, standards, and procedures to ensure accuracy and completeness. The condition observed regarding data classification relates specifically to the lack of enforcement through a formalized procedure—not to the absence of policy or its periodic review.

Information Technology Services (ITS) Information Security (InfoSec) at Edwardsville will elevate an event, discovered or reported, once investigated if it is outside of the standard deviation of tiered support business continuity events. All cases of suspected events throughout ITS publications, orientation, training, policy and point of service calls direct users to the ITS Help Desk comprehensively. Reported Phishing events can be received via the phishing email inbox and the phishing reporting button within the email client, which goes directly to ITS InfoSec for investigation and response

Because of the sensitive nature of data handled by the School of Medicine (SOM), all data is held to the same standard. Different controls are not applied based on data classification. The environment is held to the highest standard unless an exception is documented. SOM will be revising security documentation to clarify this approach.

SOM has the supporting documents about restoration steps – they are maintained separately from the actual disaster recovery plan.

ACCOUNTANT'S COMMENT:

Records provided by the University, which were reviewed and discussed during the compliance examination, did not support sufficient controls and compliance related to data privacy training at SIUE or SIUC, documented revision or approval date of SIUC retention schedules, formal employee guidance for incident reporting at SIUE, or written, step-by-step data recovery instructions at SOM.

In addition, SIUC's data protection policy lacked all or part of four (80%) of the five specific elements mandated by the Identity Protection Act (5 ILCS 179).

Further, all information at SOM is not held to the same standard or subject to the same controls regardless of the type of data. Some information used in SOM's operations, including but not limited to publicly available data such as marketing materials, some statistics and general information on SOM's website, is not sensitive and access is not, and does not need to be limited, whereas storage and access to protected classes of information must be limited to only authorized persons. Therefore, different controls are needed to identify and differentiate public versus confidential, sensitive, and protected information, and systems and controls storing and protecting non-public data must be monitored.

The concerns noted in the University's finding response were not raised in the exit conference held to discuss results of the compliance examination.

UPDATED RESPONSE:

• *Each campus of the University enhances its risk assessment procedures to specifically include addressing the risks pertaining to confidential data controls, categorization of systems, and mitigating controls for legal risk.*

SOM

• **Implemented**: No change. IT. SOM now uses an outside firm to assist with risk assessment and risk mitigation activities, which are tracked as part of that engagement.

SIUC

• **Under Study**: No change. CIO, CISO/ITGRC. SIU Carbondale has just hired new CISO and charted an IT Governance, Risk, and Compliance office to assess and redesign the ISP and associated procedures.

• *Each campus of the University identifies and evaluate data classification policies and monitoring controls, including identifying types of confidential data, systems, data owners, and evaluating the effectiveness of data controls and updating policies as needed.*

SOM

• **Under Study**: No change. IT/CISO.

SIUC
• **Under Study**: No change. CIO, CISO/ITGRC. SIU Carbondale has just hired new CISO and charted an IT Governance, Risk, and Compliance office to assess and redesign the ISP and associated procedures.

• *SIUC and SIUE implement privacy training for staff who handle Social Security Numbers (SSNs).*

SIUC
• **Implemented:** No change. CISO. SIU Carbondale does provide as part of the cybersecurity training basic PII and SSN safe handling guidelines.

• **Under Study**: No change. OGC, University Risk Management, CISO/IT GRC. Targeted privacy training for those roles where access to PII, SSN, etc. are part of daily work.

• *SIUC and SIUE implement a process for regular reviews of policies and procedures, including a documented revision date and approval date.*

SIUC
• **Implemented:** No change. CISO. SIUC OIT has an annual review process for all IT policies and procedures.

• *SIUC implement a Business Impact Analysis to identify confidential and personal information susceptible to attacks.*

SIUC
• **Under Study**: No change. CIO, CISO/ITGRC. SIU Carbondale has just hired new CISO and charted an IT Governance, Risk, and Compliance office to assess and redesign the ISP and associated procedures.

SIUE
Under Study. No change. Information Security Officers.

4. The auditors recommend the University strengthen information security controls across the University's environment and devices.

FINDING: *Information Security Related Weaknesses – This finding has been repeated since 2020.*

Southern Illinois University (University) did not maintain adequate security controls over its environment and devices.

The University maintains computer resources across its campuses for users to conduct University functions. During their examination, the auditors reviewed the controls over servers and workstations to determine if appropriate security controls had been

implemented. Although the University addressed some security related weaknesses noted in the prior examination, they noted some information security control weaknesses still existed.

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.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) and the *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Special Publication 800-171, Third Revision) published by the National Institute of Standards and Technology, Configuration and Maintenance sections, requires entities to maintain adequate security controls over their environment and devices.

University management indicated weaknesses in information security were due to limited resources and additional time needed to implement corrective action.
Failure to implement adequate security controls over the environment and devices exposes the University to increased danger of unauthorized access and the loss or corruption of critical and confidential data.

UNIVERSITY RESPONSE:
Agree. SIUC acknowledges that at the time a server was operating on an end-of-life operating system, as this was a temporary measure taken while awaiting certification from a software vendor to ensure compatibility with an application with the updated operating system. The server in question was for internal use, accessed only by a specific team, and additional security restrictions were in place. Given these controls, the associated risk was assessed to be low.

The University recognizes that the expectation for the Information Technology Security Plan is to identify specific individuals by name or role for certain security control. Responsibilities related to security, patching, and control implementation are typically distributed across teams, and individual assignments are subject to change due to role transitions, organizational restructuring, resource availability, or staff turnover. In such a dynamic environment, maintaining individual named assignments would be administratively burdensome and prone to inaccuracies. Moreover, including named individuals in the publicly available portion of the plan could inadvertently introduce risk.

To address this, the University proposes documenting these responsibilities by team or functional area, offering a more stable and scalable approach. Internal documentation will be reviewed and updated as needed, to ensure that any gaps are addressed and that accountability remains clear and traceable.

UPDATED RESPONSE:

Implemented. No change. CISO / Director of Infrastructure. SIUC has an annual review process of security controls, procedures, and policies. We are committed to continual improvement of all security controls.

SIUE
Under Study. No change. Information Security Officers.

5. The auditors recommend the University implement an access control policy and ensure coordinated University wide periodic access reviews are conducted for systems that have financial reporting information, confidential information, or are critical to University operations.

FINDING: *Lack of User Access Review – This finding has been repeated since 2022.*

Southern Illinois University (University) did not perform periodic review of access granted to users for all systems and applications.

The University reported it relied upon 84 different applications during Fiscal Year 2024, which were used for financial reporting, contained confidential information, and/or were considered critical to their operations.

During their review, the auditors noted the University (SIUC and SIUE) had not implemented an overarching access control policy requiring periodic user access reviews and had not conducted a review of users' access on an annual basis to ensure access rights were appropriate for the majority of applications identified. Further, for the two applications for which user access was reviewed, they noted:

- At SIUC, the Student Information System (SIS) user access review process had not been implemented during Fiscal Year 2024.
- SIUE conducted a SIS user access review in 2024; however, the user access review did not include documentation on who performed the user access review, when it was performed, and documentation that each user was appropriate.

This finding was first noted during the University's Fiscal Year 2022 State compliance examination. University management has been unsuccessful in implementing a corrective action plan to remedy this deficiency.

The National Institute of Standards and Technology publications *Security and Privacy Controls for Information Systems and Organizations* (NIST 800-53, Fifth Revision) and the *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Special Publication 800-171, Second Revision) Access Control sections, requires entities to develop access provisioning policies and establish controls to ensure authorized users only have needed access.

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.

Finally, the University's management team is responsible for implementing timely corrective action on all findings identified during a State compliance examination.

University management (IT) indicated the weaknesses were due to an inability to successfully engage University wide business units in supporting a detailed user access review and lack of defined roles and responsibilities for the user access review process.

Failure to periodically review users' access rights could result in inappropriate access to and manipulation of the University's data.

UNIVERSITY RESPONSE:
Agree. Implementation continues. We acknowledge a gap existed in SIUC's SIS user access review process—specifically for long-term employees whose roles remain stable and are not subject to frequent transitions. Historically, reviews focused primarily on new hires and position changes, overlooking static accounts. To address this, we developed and launched a formal SIS annual user access review process in February 2025, as part of our FY25 initiatives. This process ensures that all user accounts, including those long-standing employees, are reviewed for appropriate access levels and continued relevance. We believe this enhancement directly addresses the condition noted and will support the resolution of the related finding for the Carbondale campus.

Additionally, SIUE is currently developing a new procedural process to audit all Banner User's access each year. New procedures should be in place during FY26.

UPDATED RESPONSE:
Implemented. No change. Director of Enterprise Solutions. SIUC developed and deployed a process to improve the access control review and include the noted deficiency related to the SIS Access Review, and deployed Feb 2025.

Partially Implemented. SIUE 30% complete. December 2026 target completion. ITS UIS Director, Interim CIO.

6. The auditors recommend SIUC enhance their change management documentation requirements to include evidence of testing.

FINDING: *Lack of Change Management Controls – This finding has been repeated since 2022.*

Southern Illinois University's Carbondale campus (SIUC) did not consistently provide documented evidence that the University's Change Management policies were followed.

The University carries out its mission through the use of Information Technology (IT), including various applications. During their review of SIUC's IT general controls, the auditors noted for 5 of 5 (100%) changes sampled, evidence of testing was not documented in the change ticket.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) and the *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Special Publication 800-171, Third Revision) published by the National Institute of Standards and Technology, Configuration Management section and Configuration Change Control sections require entities to establish change management procedures to ensure changes are properly controlled.

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.

SIUC indicated that testing was performed but not formally documented in the change ticket by the approver who is responsible for validating that testing was performed to a sufficient result.

Failure to document changes to applications increases the risk that an authorized change could be put in production that was not properly tested and did not function as intended.

UNIVERSITY RESPONSE:

Agree. Implementation continues. The current change management documentation, maintained via SIUC's ticketing system, for AIS and SIS-specific changes does not include a formal statement or collection of testing evidence. While best practices dictate that no change should be promoted to production until the requester confirms satisfaction with the completed work, we acknowledge that the absence of explicit testing documentation may be viewed as a gap.

We maintain that requiring detailed testing evidence for every change is administratively burdensome and, in some cases, impractical due to the diverse nature of change requests. To address this concern, we will implement a standardized attestation of testing within the change management process. This attestation will confirm that appropriate testing has been completed and that the requestor has approved the change for production.

Additionally, we will explore options to allow the individual providing the attestation to include relevant testing documentation when appropriate. However, we emphasize that the presence or absence of formal testing documentation does not materially affect the quality of the testing or the work being performed. Our teams adhere to rigorous standards and practices that ensure changes are thoroughly validated before deployment, regardless of documentation format.

UPDATED RESPONSE:
Implemented: No change. Director of Enterprise Solutions. An attestation of testing in the change ticket is complete.

Under Study: Director of Enterprise Solutions. Formal test plan document attachment for a change ticket.

7. The auditors recommend SIUC adjust device destruction documentation tickets to include the data fields not completed in the finding.

FINDING: *Data Wiping Internal Control Weaknesses – New*

Southern Illinois University Carbondale (SIUC) had internal control weaknesses over its wiping of data from electronic systems and media.

During their testing of the University's data wiping from electronic systems, the auditors noted the following conditions at SIUC:

- For 20 of the 25 (80%) devices sampled, the method of destruction was not documented for disposed devices.
- For 25 of 25 (100%) devices sampled, the name and signature of the individual overwriting or performing the destruction of disposed surplus equipment was not documented.

The Data Security on State Computers Act (20 ILCS 450) requires the University to implement a policy to mandate all hard drives of surplus State-owned electronic data processing equipment utilized by the University to be erased, wiped, sanitized, or destroyed in a manner that prevents retrieval of sensitive data and software before being sold, donated or transferred by (i) overwriting the previously stored data on a drive or a disk at least three times or physically destroying the hard drive and (ii) certifying in writing that the overwriting process has been completed by providing the following information: (1) the serial number of the computer or other surplus electronic data processing equipment; (2) the name of the overwriting software or physical destruction process used; and (3) the name, date, and signature of the person performing the overwriting or destruction process.

The State Records Act (5 ILCS 160/8) requires the University to make and preserve records containing adequate and proper documentation of the functions, decisions, and essential transactions of the University to protect the legal and financial rights of the State and of persons directly affected by the Department's activities.

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.

Management stated they could not provide evidence of either the method of destruction or the name of the individual overwriting or performing the destruction since this information was noted on the physical destruction tag per surplus property procedures and not in the electronic ticket.

The lack of adequate electronic data management controls related to wiping data could increase the risk of unintended data exposure.

UNIVERSITY RESPONSE:
Agree. Fully implemented. SIUC affirms adherence to both SIU Procurement and State of Illinois CMS policies and standards regarding data destruction and surplus equipment handling. The current CMS process requires a physical paper tag to be affixed to each device, certifying that data has been wiped and/or physically destroyed before the device can be accepted by the CMS warehouse.

In addition to this external requirement, SIUC IT teams internally track surplus items through the University's ticketing system. We acknowledge that until recently, we did not capture the identity of the individual performing the data destruction nor the specific method used. To address this, SIUC modified its internal ticketing procedures during FY25 to include both the individual responsible and the method of destruction.

We believe this enhancement satisfies the condition noted and will support the resolution of the related finding. It is important to note, however, that this change was implemented mid-year, and as a result, some items reviewed during FY25 audit testing may still lack this information.

Finally, we emphasize that even though this information was not previously tracked in our ticketing system, the rigid standards enforced by both SIU Procurement and the State of Illinois CMS would not permit any device to be transferred to surplus property without first being properly wiped and/or physically destroyed. These procedural safeguards ensure that data destruction is consistently and effectively carried out, regardless of documentation format.

UPDATED RESPONSE:
Implemented. No change. CISO / Director of Client Services.

8. **The auditors recommend the University dedicate specific resources to complete annual reconciliations of census data and to submit certifications and potential errors identified by the required due date. They further recommend the University promptly reconcile the census data, submit the required certifications and any potential errors noted to SURS, and work with SURS to address any differences noted.**

FINDING: *Census Data Reconciliation – This finding has been repeated since 2023.*

Southern Illinois University (University) Carbondale (SIUC) did not complete its annual census data reconciliation and certifications timely.

During their testing, the auditors noted that SIUC did not complete the reconciliation of changes in State University Retirement System (SURS) member data to University records or submit the required census data reconciliation certifications for Fiscal Year 2023 data, as required by SURS, by May 31, 2024. The campus reconciliation had not been completed as of the end of Fiscal Year 2024.

In accordance with the AICPA's Audit and Accounting Guide: State and Local Governments, the State Universities Retirement System (SURS) stated employee census data should be reconciled annually by each university to a report provided by SURS and used by SURS' and CMS' actuaries. This reconciliation process helps mitigate the risk of using incomplete or inaccurate data and ensures the accuracy of reported pension and other post-employment benefit (OPEB) balances. Further, this reconciliation process ensures the completeness of employer and plan data, reduces payroll errors, confirms personnel files are up-to-date, and most importantly decreases the risks of financial misstatements. SURS requested the University to reconcile their Fiscal Year 2023 census data, certify to SURS that the reconciliation and eligibility review was completed, and report any potential data errors found by May 31, 2024.

University management stated the campus did not have sufficient resources to timely complete annual census data reconciliations and related certifications.

Failure to timely perform reconciliations of census data and to submit the required certifications could lead to reduced reliability of pension and OPEB related information and balances.

UNIVERSITY RESPONSE:
Agree. Partially implemented. SIUC, including SOM, continues to make progress in completing the SURS Census Earnings reconciliation. Completion remains a priority; staff turnover and limited resources contribute to delays in successful progress as originally planned. All other related reconciliations that are part of the SURS Census Data testing are complete aside from the earnings reconciliation. This process is very time intense, detail oriented, and takes a greater understanding of SURS/Payroll calculations and eligibility. Staff are working through this as time allows while ensuring day-to-day Payroll & Benefit processing remains the main priority. SIUC will continue to work with SOM as they complete their reconciliation of all Springfield staff. Once completed, SIUC and SOM will work with SURS to address any differences noted.

UPDATED RESPONSE:
Partially implemented. No change. 75% complete. April 1, 2026, target completion. Director of Payroll and Benefits.

9. The auditors recommend the University:

- **Review current practices to determine enhancements which can be implemented to prevent the theft or loss of computers.**
- **Evaluate and secure computers to ensure confidential information is protected.**
- **Perform and document an evaluation of data maintained on computers and ensure those containing confidential information are adequately tracked and protected with methods such as encryption.**
- **Conduct an analysis to determine if confidential information was maintained on the unlocated computers. If so, they recommend the University comply with the notification requirements of the Personal Information Protection Act.**

FINDING: *Weakness in Computer Inventory Control – This finding has been repeated since 2012.*

Southern Illinois University (University) had inadequate controls over its computer inventory.

The University was unable to locate 49 computers from Edwardsville, 226 from Carbondale, and 5 from the School of Medicine (SOM) in Springfield during their annual inventory.

Although the University had established procedures for requiring encryption on computers that could have confidential information on them, the University could not definitively indicate if the missing computers were encrypted or contained confidential information. After computers were reported missing, the University requested responsible staff to assert whether confidential information was maintained on those computers. Staff asserted that 3 machines missing from Edwardsville and 2 machines missing from Carbondale potentially contained confidential information.

The original cost of these items for the Edwardsville and Carbondale (including the Springfield location) campuses totaled $42,078 and $250,699, respectively. After the Fiscal Year 2024 inventory verification was sent to the Department of Central Management Services, 19 of the missing computers reported by Carbondale, totaling $25,155, were located.

This finding was first noted during the University's Fiscal Year 2012 State compliance examination. As such, the University has been unsuccessful in implementing corrective action to remedy this deficiency.

The State Property Control Act (30 ILCS 605/4 and 6.02) requires every responsible officer of State government to be accountable to the administrator for the supervision, control and inventory of all property under its control. In addition, the University had the responsibility to ensure that confidential information was protected from disclosure and complied with the provisions of the Personal Information Protection Act (815 ILCS 530).

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.

Finally, the University's management team is responsible for timely implementing sufficient corrective action on all findings identified during a State compliance examination.

University management stated corrective actions had not eliminated the weaknesses noted because budgetary constraints restrict the amount of manpower that can be allocated to this project.

Failure to maintain adequate controls over computer inventory has resulted in lost or stolen computer inventory and the potential for unintended exposure of confidential information.

UNIVERSITY RESPONSE:

Partially Agree. Implementation continues. Efforts are in progress and continue to improve inventory control and data protection, which show measurable progress.

Carbondale (SIUC) Property Control, based on recommendations from the Computer Inventory Management group, developed and deployed a mobile inventory application. Successfully used campus-wide during the FY25 inventory cycle, this tool aims to standardize inventory processes across all units and provide timely data to Property Control. Planned updates will further enhance the platform, with a focus on reducing item loss through a unified inventory system. Notably, use of the mobile app this fiscal year has led to the recovery of property previously reported as lost and the inability to locate, now far exceeds thefts in frequency.

SIUC Office of Information Technology (OIT) enhanced asset encryption by completing a Spring 2025 transition from two separate endpoint management products to a single unified solution supporting both Windows and Apple platforms. This change improves tracking and ensures that workstations are encrypted and reportable.

Additionally, SIUC has upgraded and streamlined its data discovery toolset in conjunction with the endpoint transition. These tools help identify, track, and, where appropriate, eliminate sensitive data from campus workstations. We acknowledge that resource limitations may prevent full identification of all sensitive data locations on workstations. Therefore, we continue to enforce full encryption as a precautionary measure, assuming sensitive data may exist.

By policy and practice, SIUC OIT secures computers through encryption and protects accounts using strong passwords, multi-factor authentication (MFA), and access control policies. Reports of lost inventory are analyzed to verify encryption status and scan results

for sensitive information. Encryption renders data unusable in the event of loss or unauthorized access to a physical device. The University complies with the Personal Information Protection Act (PIPA) when a breach is determined to have occurred; however, the loss of an encrypted machine alone does not constitute a breach. All breach determinations are made jointly by Information Technology and SIU Legal and Compliance. An analysis occurs to determine if confidential information was maintained on unlocated computers for every reported missing or stolen device. This has been standard practice for many years, with recent improvements making the process more accurate and precise.

Compensating controls are in place to mitigate any inadequacy of computer inventory controls. A zero-tolerance standard for testing inventory, along with accountability for 100% of inventory is considered a controls test failure. Many of the lost computer's pre-date data protection and encryption programs.

Note, since all domain equipment, particularly assets with high risk of loss and theft, are encrypted, then no assets contain sensitive data even when unaccountable, as encryption renders all data unusable.

ACCOUNTANT'S COMMENT:

While SIU noted above that all domain equipment is encrypted, management also stated that many lost computers pre-date encryption programs and therefore would not be encrypted. Without documentation to definitively verify that the missing machines were encrypted, there is potential that they could have contained sensitive data.

UPDATED RESPONSE:

• *Review current practices to determine enhancements which can be implemented to prevent the theft or loss of computers.*

- **Implemented**: No change. Director of Service Campus Operations / Director of Enterprise Solutions. This initiative is a joint effort between Property Control and OIT. OIT has helped develop and design inventory applications to improve tracking and locating of assets, which were deployed during the FY25 cycles, including the assignment of a custodian for each asset. We are complete on the deployment of new tracking and location applications, but analysis and improvements continue.

- **Under study**: No change. Director of Campus Service Operations, VCAF. SIU Carbondale hired a new Director of Service Campus Operations in Fall 2025, whose portfolio includes property control and inventory management and will identify additional improvements and enhancements.

- **Under study**: No change. CIO, CISO, Director of Client Services. Centralizing computer inventory responsibility to OIT and making inventory spot checks as a standard operating procedure for any desk side visit or support interaction.

• *Evaluate and secure computers to ensure confidential information is protected.*

• **Partially Implemented**: No change. 85% complete. FY28 target completion. Director of Campus Service Operations, VCAF, CIO, and CISO. Modern workstations (manufactured post-2016) with hardware encryption capabilities are secured using the operating system's native encryption tools, in accordance with established policy and practice. Older workstations manufactured prior to that timeframe cannot be encrypted. While the number of these devices on the network is minimal, most are either tied to specialized lab equipment or retained as surplus inventory. As we able to complete modernization of the fleet, we will complete the 100% encryption goal.

• *Perform and document an evaluation of data maintained on computers and ensure those containing confidential information are adequately tracked and protected with methods such as encryption.*

• Partially Implemented: No change. 75% complete. FY27 target completion. CISO/IT GRC, Director of Infrastructure. Does track and ensure workstations that can be encrypted are. In addition, data scanning tools sets such as Microsoft DLP (cloud) and Spirion Data Finder (on-premise) are used to locate confidential data. To improve these efforts in information tracking, OIT is investing in an upgraded version of Spirion that will provide the ability to tag and track data, both with on-premise and cloud-based data storage. We anticipate this will be fully in production by the end of FY27.

• *Conduct an analysis to determine if confidential information was maintained on the unlocated computers. If so, we recommend the University comply with the notification requirements of the Personal Information Protection Act.*

• Implemented: No change. CISO. This process is performed each time a computer cannot be located. Where there are indications that are PII on unencrypted workstations, we follow the requirements of PIPA.

10. The auditors recommend the University continue to monitor courses offered and approved for equivalent majors and ensure courses meeting the major panel requirements are submitted for review.

FINDING: *Noncompliance with Illinois Articulation Initiative – This has been repeated since 2020.*

Southern Illinois University (University) did not maintain a minimum of one approved course per major under the Illinois Articulation Initiative (Initiative or IAI) for some majors offered by the University.

The Initiative, through its itransfer.org website, exists to ease the transfer of students among the State's associate and baccalaureate degree granting institutions. The Initiative consists of both a General Education Core Curriculum package, where completion of the entire package at one institution is fully accepted by 108 institutions across the State, and an Initiative major, which provides general guidance for students with uncertain transfer plans.

During Fiscal Year 2024, the University did not have a minimum of one course approved by the Initiative panel included within the related Initiative major for its political science (Carbondale) or political science and early childhood (Edwardsville) degree programs.

The Illinois Articulation Initiative Act (Act) (110 ILCS 152/15) requires the University participate in the Initiative by submitting and maintaining a complete core curriculum package as well as up to four core courses in each related Initiative major, if the University has an equivalent major and courses. Major courses must be accepted by an IAI panel of college and university representatives in order to satisfy the major course requirement. Effective August 9, 2024, the Act was modified to require the Illinois Board of Higher Education, the Illinois Community College Board, and IAI to jointly determine the University's compliance if an equivalent major and/or courses aligning with the major panel's descriptor and course criteria don't exist.

The finding was first noted during the University's Fiscal Year 2020 State compliance examination. As such, the University has been unsuccessful in implementing corrective actions to remedy this deficiency.

Management at the Carbondale campus stated they did not offer an Initiative approved course for its political science major due to a delay in submission while the instructor was on sabbatical.

Edwardsville campus management stated Initiative approved courses were not offered due to the University not currently offering courses that align with the specific IAI descriptors for political science or early childhood education due to various factors such as differing academic priorities.

Failure to fully participate in the Initiative by maintaining at least one course approved by the IAI panel per Initiative major, when an equivalent major and courses exist, could hinder students looking to transfer to other institutions and represents noncompliance with State law.

UNIVERSITY RESPONSE:

Partly Agree. Implementation continues. The SIUC is working with faculty and leadership to identify and implement an appropriate 2nd-year level course. We anticipate a Fall 2025 submission of such a course.

At present, Southern Illinois University Edwardsville (SIUE) does not offer a course that directly matches the IAI major course descriptors in question, nor has IAI indicated an intent to broaden those descriptors to reflect the diversity of curricular approaches across institutions. The statutory language on this matter remains open to interpretation. SIUE maintains that we are in compliance with the intent of the law, as we do not offer an existing equivalent course in our catalog that would necessitate alignment.

Historically, our understanding—consistent with IAI's original purpose—has been that four-year institutions are expected to accept IAI major recommendations in transfer where appropriate but are not obligated to modify existing curricula or develop new courses solely to conform to IAI descriptors. When we offer equivalent courses, we submit them for IAI approval in accordance with policy, and we consistently accept IAI-approved courses in transfer. When no direct equivalent exists, we award discipline-specific elective credit in keeping with statewide transfer guidelines.

While we are aware that recent audit findings have raised questions, we remain cautious about moving toward either of the following approaches:

- Altering existing courses to match IAI content solely for compliance purposes, or
- Creating entirely new courses that duplicate content outside of our curricular offerings.

We continue to engage in dialogue with IAI partners and state agencies to ensure compliance while preserving institutional flexibility and academic rigor.

Language of the law in question (highlighted section):
Failure to fully participate in the Initiative by maintaining at least one course approved by the IAI panel per Initiative major, when an equivalent major and courses exist, could hinder students looking to transfer to other institutions and represents noncompliance with State law. (Finding Code No. 2024-010, 2023-011, 2022-020, 2021-011, 2020-014)

ACCOUNTANT'S COMMENT:
The University was unable to provide documentation supporting they were in compliance as of the date of their finding response.

UPDATED RESPONSE:
SIUC
Partially Implemented. No change. 50% completion. Director of University Core Curriculum. SIUC has created a Political Science course to meet the one remaining area in which we did not have at least one course. This course has been submitted to our Provost office for review and approval for the 2026-2027 catalog; and will be submitted to the IAI POLS Panel for review. If approved by IAI POLS Major Panel to meet the PLS913 designation we will be fully compliant.

SIUE
Partially Implemented. No change. 55% completion. Transfer Coordinator. FY27 target completion. SIUE continues to monitor course offerings and approvals via IAI Major Panels. Over the years, we have submitted course offerings for approval to IAI Major Panels in the areas of Political Science and Early Childhood Education. The IAI Major Panel denied our requests for the appropriate IAI descriptors in these discipline-specific courses.

Leadership and the listed departments continue to work on curriculum reviews including current academic prioritization curriculum revisions that we anticipate will lead to better alignment with appropriate IAI descriptors. We anticipate finalizing prioritization revisions in Academic Year 2026-2027. Subsequently, SIUE Transfer Coordinator will submit appropriate courses to the IAI Major Panels for review.

11. The auditors recommend SIUC implement internal controls to ensure the submission, retention and periodic re-evaluation of the plan, and the assignment of responsible individuals and back up staff to ensure implementation and monitoring of the plan for compliance.

FINDING: *Internal Control Weaknesses over Waste Management Plan – This finding has been repeated since 2023.*

Southern Illinois University (University) Carbondale (SIUC) lacked sufficient internal controls over their solid waste management plan during Fiscal Year 2024.

SIUC could not provide their solid waste reduction plan and, as of the end of the audit period, could not determine such a plan had been submitted to the Environmental Protection Agency (EPA) for review and approval since 2010.

The Illinois Solid Waste Management Act (415 ILCS 20/3.1) requires each State-supported institution of higher learning to develop a comprehensive waste reduction plan covering a period of 10 years which addresses the management of solid waste generated by academic, administrative, student housing and other institutional functions. The Act requires a waste reduction plan to address existing waste generation by volume, waste composition, existing waste reduction and recycling activities, waste collection and disposal costs, future waste management methods, and specific goals to reduce the amount of waste generated that is subject to landfill disposal. The Act states that the plan shall be updated every 5 years, and any proposed amendments to the plan shall be submitted for review and approval to the EPA.

The State Records Act (Act) (5 ILCS 160/3) states all records created or received by or under the authority of or coming into the custody, control, or possession of public officials of this State in the course of their public duties are the property of the State. These records may not be mutilated, destroyed, transferred, removed, or otherwise damaged or disposed of, in whole or in part, except as provided by law. The Act (5 ILCS 160/8) further requires each agency to make and preserve records containing adequate and proper documentation designed to furnish information to protect the legal and financial rights of the State and of persons directly affected by the agency's activities.

SIUC management stated this exception was due to staff turnover.
Failure to maintain adequate internal controls to ensure an approved ten-year solid waste reduction plan has been submitted, internally maintained and followed may prevent achievement of the Act's public policy by the campus, decrease public accountability, and prevent review of University waste management practices by oversight bodies.

UNIVERSITY RESPONSE:
Agree. Implemented. SIUC submitted a waste management plan on April 1, 2025, to comply with the five-year update pursuant to 415 ILCS 20/3.1, and Illinois Environmental Protection Agency confirmed receipt. SIUC's Director of Facilities and Energy Management files this report. Additionally, SIUC created a Waste Management Planning Committee. Files, meeting minutes, and all correspondence with the committee are held in a shared folder to prevent the loss of information due to changes in staffing.

UPDATED RESPONSE:
Implemented. No change, Director of Facilities and Energy Management.

12. The auditors recommend the University work with designated parties to ensure appointment of and participation by Board members. They further recommend the University ensure the responsible staff are informed and receive training as needed to satisfy statutory mandates for the Advisory Board.

FINDING: *Illinois Ethanol Research Advisory Board – This finding has been repeated since 2015.*

Southern Illinois University (University) did not manage the National Corn-to-Ethanol Research Pilot Plant (Pilot Plant) under the review and guidance of the Illinois Ethanol Research Advisory Board (Advisory Board) as mandated by law.

During Fiscal Year 2024, the University held a joint meeting of the Advisory Board and a combined group of stakeholders it identified, rather than just the Advisory Board required by State statute, to provide review and guidance to the University Board of Trustees to assist in operating and managing the Pilot Plant. A quorum of seven advisory board members was not achieved. Of the 34 participants in the annual meeting, it was attended by only one of the Board members designated by law, five representatives of Board member's organizations who did not meet the statutory requirement, and 28 other individuals. Since Advisory Board members constituted a minority of meeting participants and a quorum was not present, the Pilot Plant was, in essence, managed under the review and guidance of stakeholders identified by the University rather than the Advisory Board members mandated by State law.

During Fiscal Year 2024, the Pilot Plant expended $645,200 and employed 27 personnel, which consisted of 11 full-time, 7 part-time and 9 students.

The Southern Illinois University Management Act (Act) (110 ILCS 520/6.5) requires the University Board of Trustees to operate and manage the Pilot Plant for the purpose of reducing the costs of producing ethanol through the development and commercialization of new production technologies, equipment, processes, feedstocks, and new value-added co-products and by-products. The Act states this work shall be conducted under the review and guidance of the Advisory Board.

The Act (110 ILCS 520/6.6) established the Advisory Board, consisting of six at-large members, as well as eight designated agency directors, association presidents, and university deans who hold positions on the Board by virtue of their positions as the officers designated in statute. The Act also states 7 members of the Advisory Board constitutes a quorum.

The Act states the Advisory Board shall meet at least annually and have the following duties:

- Review of annual operating plans and budget of the Pilot Plant.
- Advise on research and development priorities and projects to be carried out at the Pilot Plant.
- Advise on policies and procedures regarding the management and operation of the Pilot Plant, which may include contracts, project selection, and personnel issues.
- Develop bylaws.
- Submit a final report to the Governor and General Assembly outlining the progress and accomplishments made during the year along with a financial report for the year; and
- Establish and operate the National Corn-to-Ethanol Research Center of Excellence with purposes and goals including conducting research, providing training, consulting, developing demonstration projects, and service as an independent resource to the ethanol industry.

This finding was first noted during the University's Fiscal Year 2015 State Compliance examination, ten years ago. As such, the University has been unsuccessful in implementing corrective action to remedy this deficiency. The University's management team is responsible for implementing timely corrective action on all findings identified during a State compliance examination.

University management indicated the exceptions related to the Advisory Board occurred because a quorum of the board members was not achieved at the meeting. The auditors also noted difficulties in getting Board members to attend the annual meeting and an insufficient understanding of statutory requirements.

Failure to comply with all provisions of the Act prohibits the University's ability to manage the Pilot Plant as envisioned by the General Assembly and undermines the authority of the legislature.

UNIVERSITY RESPONSE:

Agree. Implemented. The National Corn to Ethanol Research Center (Pilot Plant) agrees to conduct its annual stakeholders meeting in accordance with the Open Meetings Act (OMA) and will retain minutes of such meetings to document the duties performed by the Advisory Board. Responsible parties completed the necessary OMA training.

The FY25 Illinois Ethanol Research Advisory Board meeting, held on Monday, November 18, 2024, was held in accordance with the Open Meetings Act. Notice of the meeting was posted on November 11, 2024, on the front entrance to NCERC and on the NCERC website. The SIU President and Advisory Board Chair presided over the meeting. Minutes and a list of attendees were recorded and will be retained.

UPDATED RESPONSE:
Implemented. No change. Executive Director of NCERC.

13. The auditors recommend the University work with SURS to correct the error within the system and ensure that all dates are accurately entered moving forward.

FINDING: *Inaccurate Reporting of Leave Time for Retiree – New*

Southern Illinois University Edwardsville (SIUE) did not accurately report the number of unused sick leave days to the State University Retirement System (SURS).

During testing of the retirement population for SIUE, auditors noted one out of eighteen (6%) employees tested who retired from service during fiscal year 2024 did not have the number of unused sick leave days per the SIUE system align with the amount reported to SURS. In this instance, unused sick days were overreported by 1.38 days. The employer (SIUE) did not accurately certify to the board the number of days of unused sick leave accrued to the participant's credit on the date that the participant's status as an employee terminated accurately.

The Illinois Pension Code (40 ILCS 5/15-113.4) states a person who is an employee under this System or one of the other systems subject to Article 20 of this Code within 60 days immediately preceding the date on which his or her retirement annuity begins, is entitled to credit for service for that portion of unused sick leave earned in the course of employment with an employer and credited on the date of termination of employment by an employer for which payment is not received. Each employer shall certify to the board the number of days of unused sick leave accrued to the participant's credit on the date that the participant's status as an employee terminated.

University management indicated the inaccuracy occurred due to human error.

Failure to accurately report unused sick leave days to SURS could result in the retiree being paid an inappropriate amount by the SURS system and may impact the accuracy of financial data.

UNIVERSITY RESPONSE:
Agree. Implemented. The University corrected the error in December 2024 and will continue to work with SURS to ensure that information is correctly entered moving forward.

UPDATED RESPONSE:
Implemented. No change. Director of Human Resources.

14. The auditors recommend the University ensure it timely reports all required information to oversight bodies.

FINDING: *Noncompliance with the Developmental Education Reform Act – New*

Southern Illinois University (University) Carbondale (SIUC) did not offer or explain their decision not to offer developmental education coursework as part of developmental education reform in English, nor did it report developmental education models or detailed plans to improve outcomes for students insufficiently prepared in mathematics.

We noted:

- SIUC did not offer English developmental education coursework, and did not report details or support to the Illinois Board of Higher Education (IBHE) regarding its decision not to offer developmental education coursework and the pathways available to students deemed to be insufficiently prepared for introductory college-level English coursework.
- SIUC did not report to IBHE all required details of its developmental education reform plans for mathematics, including a description of the current developmental education models offered, the basis of the evidence and associated data considered, detailed plans for scaling reforms and improving outcomes for students, and details about the expected improvements in educational outcomes for Black students as a result of the proposed reforms.

During Fiscal Year 2024, 280 (11%) and 194 (29%) students enrolled at SIUC were reported to be insufficiently prepared for college-level coursework in English and mathematics, respectively.

The Developmental Education Reform Act (Act) (110 ILCS 175/100-30) required the University to submit to the Board of Higher Education its institutional plan for scaling evidence-based developmental education reforms to maximize the probability that a student will be placed in and successfully complete introductory college-level English language or mathematics coursework within 2 semesters at the institution. The Act required the University's plan include a description of the current developmental education models offered, the basis of the evidence and associated data considered, baseline data and benchmarks for progress, detailed plans for scaling reforms and improving outcomes for students, and details about the expected improvements in educational outcomes for Black students as a result of the proposed reforms. If the institution did not offer developmental education coursework, the Act required the University to provide details regarding its decision not to offer developmental education coursework and the pathways that were available to students deemed to be insufficiently prepared for introductory college-level English language or mathematics coursework.

University management indicated their report to IBHE lacked the required details regarding its decision to not offer developmental education coursework and the pathways that are available to insufficiently prepared students due to still being in the process of actively exploring a corequisite model to offer appropriate coursework. Management stated some required details of its developmental education reform plans for mathematics were omitted from the report submitted to IBHE due to the University still being in the process of actively working towards creating a new placement strategy.

Failure to report to IBHE details of its decision to not offer developmental education coursework and the pathways available to insufficiently prepared students in English, and details of developmental education reform plans for mathematics may reduce transparency, undermine accountability, and limit information for oversight bodies to evaluate SIUC's implementation plan.

UNIVERSITY RESPONSE:

Agree. Partially implemented. SIUC's Summer Opportunity Initiative provides summer bridge courses and academic support to students who show potential for college-level work but do not meet regular University admissions requirements. The proposed action is to include ENGL 100 in the summer prior to the start of the freshmen year to prepare students for ENGL 101 English Composition I. This early intervention model reflects a proactive approach to improving student readiness and retention.

The University is actively exploring a corequisite model, in which students would receive targeted writing support while enrolled in English 101. This support may include supplemental instruction, additional class sessions, writing workshops, or individualized tutoring—all designed to reinforce key skills while students engage in credit-bearing coursework. Corequisite models have been shown to improve pass rates and accelerate progress toward degree completion, particularly for students from underserved backgrounds.

To further strengthen academic support structures, SIUC will implement a new Early Alert system beginning in Fall 2025. This system will enable faculty teaching high-impact, foundational courses, especially ENGL 101—to submit early progress reports for students who exhibit signs of academic struggle. These reports will trigger timely interventions, connecting students to tutoring, mentoring, advising, and other wraparound services.

The Early Alert initiative is designed with equity in mind, recognizing that many underrepresented students, including first-generation college students, may be less likely to seek help independently when they encounter academic challenges.

Together, these efforts reflect SIUC's commitment to student success through multiple, integrated pathways of academic support. Although the university has not reinstated traditional developmental education courses, it continues to evolve its strategies in alignment with national best practice prioritizing acceleration, early intervention, and inclusive support to help all students succeed in college-level coursework.

The University acknowledges the importance of timely reporting to oversight bodies and appreciates the recommendation. To strengthen our reporting processes, the Associate Provost for Academic Program office will manage all correspondence and work with appropriate internal units to ensure that required reports are submitted accurately and on time. This centralized approach will help improve coordination and ensure accountability moving forward.

UPDATED RESPONSE:

Partially Implemented. 0% complete. Fall 2026 target completion. Associate Provost for Academic Programs.

Under Study. Coordinator of the Writing Studies Program. Agree. Partially implemented. SIUC's Summer Opportunity Initiative provides summer bridge courses and academic support to students who show potential for college-level work but do not meet regular University admissions requirements. The proposed action is to include ENGL 100 in the summer prior to the start of the freshmen year to prepare students for ENGL 101 English Composition I. This early intervention model reflects a proactive approach to improving student readiness and retention.

Under Study. No change. Coordinator of the Writing Studies Program. The University is actively exploring a corequisite model, in which students would receive targeted writing support while enrolled in English 101. This support may include supplemental instruction, additional class sessions, writing workshops, or individualized tutoring—all designed to reinforce key skills while students engage in credit-bearing coursework. Corequisite models have been shown to improve pass rates and accelerate progress toward degree completion, particularly for students from underserved backgrounds.

Implemented. No change. Provost for Student Success. To further strengthen academic support structures, SIUC will implement a new Early Alert system beginning in Fall 2025. This system will enable faculty teaching high-impact, foundational courses, especially ENGL 101—to submit early progress reports for students who exhibit signs of academic struggle. These reports will trigger timely interventions, connecting students to tutoring, mentoring, advising, and other wraparound services. The Early Alert initiative is designed with equity in mind, recognizing that many underrepresented students, including first-generation college students, may be less likely to seek help independently when they encounter academic challenges.

Together, these efforts reflect SIUC’s commitment to student success through multiple, integrated pathways of academic support. Although the university has not reinstated traditional developmental education courses, it continues to evolve its strategies in alignment with national best practice prioritizing acceleration, early intervention, and inclusive support to help all students succeed in college-level coursework.

Implemented. No change. Provost for Academic Programs. The University acknowledges the importance of timely reporting to oversight bodies and appreciates the recommendation. To strengthen our reporting processes, the Associate Provost for Academic Program office will manage all correspondence and work with appropriate

internal units to ensure that required reports are submitted accurately and on time. This centralized approach will help improve coordination and ensure accountability moving forward.

Emergency Purchases

The Illinois Procurement Code (30 ILCS 500/) states, "It is declared to be the policy of the state that the principles of competitive bidding and economical procurement practices shall be applicable to all purchases and contracts…." The law also recognizes that there will be emergency situations when it will be impossible to conduct bidding. It provides a general exemption when there exists a threat to public health or public safety, or when immediate expenditure is necessary for repairs to state property in order to protect against further loss of or damage to state property, to prevent or minimize serious disruption in critical state services that affect health, safety, or collection of substantial state revenues, or to ensure the integrity of state records; provided, however that the term of the emergency purchase shall not exceed 90 days. A contract may be extended beyond 90 days if the chief procurement officer determines additional time is necessary and that the contract scope and duration are limited to the emergency. Prior to the execution of the extension, the chief procurement officer must hold a public hearing and provide written justification for all emergency contracts. Members of the public may present testimony.

Notice of all emergency procurement shall be provided to the Procurement Policy Board and published in the online electronic Bulletin no later than five business days after the contract is awarded. Notice of intent to extend an emergency contract shall be provided to the Procurement Policy Board and published in the online electronic Bulletin at least 14 days before the public hearing.

A chief procurement officer making such emergency purchases is required to file a statement with the Procurement Policy Board and the Auditor General to set forth the circumstance requiring the emergency purchase. The Legislative Audit Commission receives quarterly reports of all emergency purchases from the Office of the Auditor General. The Legislative Audit Commission is directed to review the purchases and to comment on abuses of the exemption.

SIU had one emergency purchase in the third quarter of FY24 for an actual cost of $328,990 in state funds for replacement electrical equipment. They had two emergency purchases in the fourth quarter of FY24. The first for an estimated cost of $566,068 in state funds for roof replacements due to storm damage while waiting for insurance reimbursement. The second for an actual cost of $25,438.83 in other funds for a location to provide medical care to an underserved population on the northern side of Springfield, approved by the Health Resources and Services Administration.

Headquarters Designations

The State Finance Act requires all state agencies to make semiannual headquarters reports to the Legislative Audit Commission. Each state agency is required to file reports

of all its officers and employees for whom official headquarters have been designated at any location other than that at which official duties require them to spend the largest part of their working time.

As of July 2024, SIU had 0 employees assigned to locations others than official headquarters.