

**State Employees' Retirement System
of Illinois**
(a component unit of the State of Illinois)

State Compliance Examination

For the Two Years Ended June 30, 2023
Performed as Special Assistant Auditors for
the Auditor General, State of Illinois

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)
State Compliance Examination**

For the Two Years Ended June 30, 2023

Table of Contents

State Compliance Examination Report

	Page
System Officials and Governing Board Members	1
Management Assertion Letter	3
Compliance Report	
Summary	4
Independent Accountant's Report on State Compliance and on Internal Control Over Compliance	6
Schedule of Findings	
Current Findings	9
Prior Finding Not Repeated	12

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)
State Compliance Examination**

For the Two Years Ended June 30, 2023

System Officials

Executive Secretary	Timothy B. Blair
Accounting Division Manager	Kristi Conrad, Acting (1/1/2023 – present) Alan Fowler, CPA (Through 12/31/2022)
Legal Counsel	Samantha Goetz (10/3/2022 – present) Vacant (2/05/2022 – 10/2/2022) James Stivers (Through 2/04/2022)
Chief Internal Auditor	Casey Evans

Governing Board Members

Chair of the Board	Susana Mendoza
Trustee (Vice-Chair of the Board)	Vacant (5/1/2024 – present) David Morris (Through – 4/30/2024)
Trustee	Danny Silverthorn
Trustee	Mohamad Nasir (5/22/2023 – present) Vacant (10/25/2022 – 5/21/2023) Carl A. Jenkins (Through – 10/24/2022)
Trustee	Jeremy Hawk
Trustee	Jack Matthews (7/16/2021 – present) Vacant (7/1/2021 – 7/15/2021)
Trustee	Arnold Black** (4/26/2022 – present) Vacant (01/01/2022 – 04/25/2022) Stephen Miltons (04/19/2016 – 12/31/2022)
Trustee	Melverta Wilkins (2/28/2022 – present) Vacant (10/15/2015 – 02/27/2022)
Trustee	John Tilden
Trustee	Barbara J.C. Baird
Trustee	Jameson Ramirez (12/13/2021 – present) Vacant (7/1/2021 – 12/12/2021)
Trustee	Mona Naser (11/27/2023 – present) Mark Donovan (12/21/2021 – 11/26/2023) Vacant (7/1/2021 – 12/20/2021)

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)
State Compliance Examination**

For the Two Years Ended June 30, 2023

Trustee

Ray Koenig III (2/14/2022 – present)
Vacant (7/28/2021 – 2/13/2024)
Renee Friedman (7/1/2021 – 7/27/2021)

** Vice-Chair of the Board, effective 5/1/2024, after the retirement of the former Vice-Chair.

Office Locations

Springfield Office

2101 South Veterans Parkway
P.O. Box 19255
Springfield, Illinois 62794-9255

Chicago Office

State of Illinois Building
160 North LaSalle Street, Suite N725
Chicago, Illinois 60601



State Employees' Retirement System

srs.illinois.gov

MANAGEMENT ASSERTION LETTER

June 26, 2024

RSM US LLP
1450 American Lane
Suite 1400
Schaumburg, IL 60173

Ladies and Gentlemen:

We are responsible for the identification of, and compliance with, all aspects of laws, regulations, contracts, or grant agreements that could have a material effect on the operations of the State Employees' Retirement System (System). We are responsible for and we have established and maintained an effective system of internal controls over compliance requirements. We have performed an evaluation of the System's compliance with the following specified requirements during the two-year period ended June 30, 2023. Based on this evaluation, we assert that during the years ended June 30, 2022 and June 30, 2023, the System has materially complied with the specified requirements below.

- A. The System has obligated, expended, received and used public funds of the State in accordance with the purpose for which funds have been appropriated or otherwise authorized by law.
- B. The System has obligated, expended, received and used public funds of the State in accordance with any limitations, restrictions, conditions or mandatory directions imposed by law upon such obligation, expenditure, receipt, or use.
- C. The System has complied, in all material respects, with applicable laws and regulations, including the State uniform accounting system, in its financial and fiscal operations.
- D. State revenues and receipts collected by the System are in accordance with applicable laws and regulations and the accounting and recordkeeping of such revenues and receipts is fair, accurate, and in accordance with law.
- E. Money or negotiable securities or similar assets handled by the System on behalf of the State or held in trust by the System have been properly and legally administered, and the accounting and recordkeeping relating thereto is proper, accurate and in accordance with law.

Yours truly,

State Employees' Retirement System of Illinois

SIGNED ORIGINAL ON FILE

Timothy B. Blair / Executive Secretary

SIGNED ORIGINAL ON FILE

Kristi Conrad, CPA, Chief Fiscal Officer

SIGNED ORIGINAL ON FILE

Samantha Goetz, General Counsel

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)
State Compliance Examination**

For the Two Years Ended June 30, 2023

State Compliance Report

Summary

The State compliance testing performed during this examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants; the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States; the Illinois State Auditing Act (Act); and the *Audit Guide*.

Accountant's Report

The Independent Accountant's Report on State Compliance and on Internal Control Over Compliance does not contain scope limitations, disclaimers or other significant non-standard language.

Summary of Findings

Number of	Current Report	Prior Report
Findings	3	6
Repeated findings	1	2
Prior recommendations implemented or not repeated	5	1

Schedule of Findings

<u>Item No.</u>	<u>Page</u>	<u>Last/First Reported</u>	<u>Description</u>	<u>Finding Type</u>
-----------------	-------------	----------------------------	--------------------	---------------------

Current Findings

2023-001	9	New	Inadequate Controls over Security Incident and Vulnerability Management	Significant Deficiency and Noncompliance
2023-002	10	2021/2020	Inadequate Internal Controls over Access to Information Systems	Significant Deficiency and Noncompliance
2023-003	11	New	Inadequate Controls over Change Management	Significant Deficiency and Noncompliance

Prior Findings Not Repeated

A	12	2021/2016	Board of Trustees Vacancy
B	12	2021/2021	Lack of Adequate Controls over the Review of Internal Controls for Service Providers
C	12	2021/2021	Weaknesses in Cybersecurity Programs and Practices
D	12	2021/2021	Disaster Recovery Planning Weaknesses
E	13	2021/2021	Lack of Agreement to Ensure Compliance with IT Security Requirements

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)
State Compliance Examination**

For the Two Years Ended June 30, 2023

State Compliance Report (Continued)

Exit Conference

The System waived an exit conference in a correspondence from Casey Evans, Chief Internal Auditor, on May 28, 2024. The responses to the recommendations were provided by Casey Evans, Chief Internal Auditor, in a correspondence dated June 4, 2024.

**Independent Accountant's Report
on State Compliance and on Internal Control Over Compliance**

RSM US LLP

Honorable Frank J. Mautino
Auditor General
State of Illinois

Board of Trustees
State Employees' Retirement System of Illinois

Report on State Compliance

As Special Assistant Auditors for the Auditor General, we have examined compliance by the State Employees' Retirement System of Illinois (System) with the specified requirements listed below, as more fully described in the *Audit Guide for Financial Audits and Compliance Attestation Engagements of Illinois State Agencies (Audit Guide)* as adopted by the Auditor General, during the two years ended June 30, 2023. Management of the System is responsible for compliance with the specified requirements. Our responsibility is to express an opinion on the System's compliance with the specified requirements based on our examination.

The specified requirements are:

- A. The System has obligated, expended, received, and used public funds of the State in accordance with the purpose for which such funds have been appropriated or otherwise authorized by law.
- B. The System has obligated, expended, received, and used public funds of the State in accordance with any limitations, restrictions, conditions, or mandatory directions imposed by law upon such obligation, expenditure, receipt, or use.
- C. The System has complied, in all material respects, with applicable laws and regulations, including the State uniform accounting system, in its financial and fiscal operations.
- D. State revenues and receipts collected by the System are in accordance with applicable laws and regulations and the accounting and recordkeeping of such revenues and receipts is fair, accurate, and in accordance with law.
- E. Money or negotiable securities or similar assets handled by the System on behalf of the State or held in trust by the System have been properly and legally administered and the accounting and recordkeeping relating thereto is proper, accurate, and in accordance with law.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the Illinois State Auditing Act (Act), and the *Audit Guide*. Those standards, the Act, and the *Audit Guide* require that we plan and perform the examination to obtain reasonable assurance about whether the System complied, in all material respects, with the specified requirements referenced above. An examination involves performing procedures to obtain evidence about whether the System complied with the specified requirements. The nature, timing, and extent of the procedures selected depend on our judgement, including an assessment of the risks of material noncompliance, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination does not provide a legal determination on the System's compliance with the specified requirements.

In our opinion, the System complied, in all material respects, with the specified requirements during the two years ended June 30, 2023. However, the results of our procedures disclosed instances of noncompliance with the specified requirements, which are required to be reported in accordance with criteria established by the *Audit Guide* and are described in the accompanying Schedule of Findings as items 2023-001 through 2023-003.

The System's responses to the compliance findings identified in our examination are described in the accompanying Schedule of Findings. The System's responses were not subjected to the procedures applied in the examination and, accordingly, we express no opinion on the responses.

The purpose of this report is solely to describe the scope of our testing and the results of that testing in accordance with the requirements of the *Audit Guide*. Accordingly, this report is not suitable for any other purpose.

Report on Internal Control Over Compliance

Management of the System is responsible for establishing and maintaining effective internal control over compliance with the specified requirements (internal control). In planning and performing our examination, we considered the System's internal control over the specified requirements as a basis for designing the examination procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the System's compliance with the specified requirements and to test and report on the System's internal control in accordance with the *Audit Guide*, but not for the purpose of expressing an opinion on the effectiveness of the System's internal control. Accordingly, we do not express an opinion on the effectiveness of the System's internal control.

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

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that have not been identified. We did not identify any deficiencies in internal control that we consider to be material weaknesses. However, we did identify certain deficiencies in internal control, described in the accompanying Schedule of Findings as items 2023-001 through 2023-003 that we consider to be significant deficiencies.

As required by the *Audit Guide*, immaterial findings excluded from this report have been reported in a separate letter.

The System's responses to the internal control findings identified in our examination are described in the accompanying Schedule of Findings. The System's responses were not subjected to the procedures applied in the examination and, accordingly, we express no opinion on the responses.

The purpose of this report is solely to describe the scope of our testing of internal control and the results of that testing based on the requirements of the *Audit Guide*. Accordingly, this report is not suitable for any other purpose.

SIGNED ORIGINAL ON FILE

Schaumburg, Illinois
June 26, 2024

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)**

**Schedule of Findings – State Compliance
For the Two Years Ended June 30, 2023**

Finding No. 2023-001 Inadequate Controls over Security Incident and Vulnerability Management

The State Employees' Retirement System of Illinois (System) had not implemented adequate controls related to security incident and vulnerability management.

In order to meet its primary goal of “providing an orderly means whereby aged or disabled employees may be retired from active service without prejudice or hardship”, the System utilized several Information Technology (IT) applications which contained confidential and personal information.

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 our examination of the System's cybersecurity program, practices, and control of confidential information we noted the System had not established a formal policy or procedure to review and ensure security incidents identified involving the System's systems or data were fully remediated and related vulnerabilities were assessed.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the System 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) published by National Institute of Standards and Technology (NIST), requires entities to consider incident and vulnerability management practices to ensure the security of their applications, data, and continued business mission.

System management indicated the lack of controls was due to oversight.

The lack of adequate security incident and vulnerability management programs and practices could result in unidentified risk and vulnerabilities, which could ultimately lead to the System's volumes of personally identifiable information being susceptible to cyber-attacks and unauthorized disclosure. (Finding Code No. 2023-001)

Recommendation:

We recommend the System establish and implement a formal policy or procedure to review and ensure incidents identified involving the System's systems or data are fully remediated and that related vulnerabilities are assessed.

System Response:

The System agrees with the finding. The System's Security Committee will implement a formal policy and procedures over incident and vulnerability management.

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)**

**Schedule of Findings – State Compliance (Continued)
For the Two Years Ended June 30, 2023**

Finding No. 2023-002 Inadequate Internal Controls over Access to Information Systems

The State Employees' Retirement System of Illinois (System) did not have adequate controls in place over user access to its Information Technology (IT) systems.

During the compliance examination, the System utilized a combination of systems administered both internally as well as externally. During a review of both internal and external systems, we noted:

- The System did not retain evidence of internal or external security reviews performed during the examination period.
- 7 of 238 (3%) user accounts maintained access to systems after the users' separations.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the System 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) published by the National Institute of Standards and Technology (NIST), Access Control section, requires entities to develop access provisioning policies and procedures and ensure access is provided on a needed basis and removed timely.

System management indicated the lack of evidence retention was due to not having a formalized process in place to document and perform the security reviews. Additionally, management indicated users retaining access to the system after their separation was due to lack of oversight.

Failure to regularly monitor and remove access puts the System at risk of unauthorized access to its information systems. (Finding Code No. 2023-002, 2021-002, 2020-003)

Recommendation

We recommend the System perform and document security reviews to ensure that continued monitoring is being performed and possible changes or updates to access rights are being made. In addition, we recommend the System implement controls to ensure users' access is timely removed after separation.

System Response

The System agrees with the finding. The System will revise procedures of access control and maintain evidence of the access reviews. Further, the System will work to ensure that all users are timely removed from all applications after separation.

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)**

**Schedule of Findings – State Compliance (Continued)
For the Two Years Ended June 30, 2023**

Finding No. 2023-003 Inadequate Controls over Change Management

The State Employees' Retirement System of Illinois (System) had not implemented adequate controls over change management.

During the compliance examination, we noted the System utilizes a combination of systems administered both internally as well as externally. These systems and applications are used in operations of the State Employees' Retirement System of Illinois, as well as for the Judges' Retirement System of the State of Illinois and the General Assembly Retirement System of the State of Illinois. During our examination procedures we noted the following:

- For a specific application, we requested the System provide documentation of changes going through the change management process. However, for 25 of 25 individual changes tested (100%), the System was unable to provide formal documentation of approval and segregation of duties between developers and promoters of changes to the application.
- For another specific application, we requested the System provide a complete and accurate listing of changes. The System provided a listing but was unable to provide evidence to document the completeness and accuracy of the listing. We did perform examination procedures on the listing provided and did not identify any specific exceptions.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the System to establish and maintain a system, or systems, of internal fiscal controls to provide assurance funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Configuration Change Control Section, promotes controls for ensuring mechanisms exist to prohibit unauthorized changes to systems within the organization.

System management indicated the lack of controls were due to oversight.

Failure to maintain adequate controls over change management could result in unauthorized changes to existing systems. (Finding Code No. 2023-003)

Recommendation:

We recommend the System establish and maintain controls over change management to ensure changes are adequately authorized, developed, tested, and documented.

System Response:

The System agrees with the finding. The System will work to implement additional controls over change management and retain documentation for all system changes.

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)**

**Schedule of Findings – State Compliance (Continued)
For the Two Years Ended June 30, 2023**

Prior Findings Not Repeated

A. Board of Trustees Vacancy

During the previous examination, the State Employees' Retirement System of Illinois (System) had vacancies in four of its thirteen required trustees of the Board. One vacancy had existed for more than six years as of June 30, 2021.

During the current examination period, we noted the Governor's office officially made four appointments to fill all the vacancies. In addition, during our testing procedures, we noted the board was composed of required representation as of June 30, 2023. (Finding Code No. 2021-001, 2020-001, 2019-001, 2018-001, 2017-002, 2016-003)

B. Lack of Adequate Controls over the Review of Internal Controls for Service Providers

During the previous examination, the State Employees' Retirement System of Illinois (System) did not implement adequate internal controls over its service providers.

During the current examination, our testing indicated the System only used one service provider, the Department of Innovation and Technology (DoIT), and was making improvements in reviewing the internal controls for DoIT. (Finding Code No. 2021-003)

C. Weaknesses in Cybersecurity Programs and Practices

During the previous examination, the State Employees' Retirement System of Illinois (System) did not implement adequate internal controls related to cybersecurity programs, practices and control of confidential information.

During the current examination, our testing indicated the System made substantial improvements in its programs and practices. However, the System did not correct an issue related to security incident and vulnerability management. As such, this issue was reported as Finding 2023-001 in the System's Compliance Examination Report. (Finding Code No. 2021-004)

D. Disaster Recover Planning Weaknesses

During the previous examination, the State Employees' Retirement System of Illinois (System) did not ensure that proper Disaster Recovery policies and procedure were in place and reviewed to ensure the System's environment was protected.

During the current examination, our testing indicated the System made substantial improvements in its Disaster Recovery programs and practices. (Finding Code No. 2021-005)

**State Employees' Retirement System of Illinois
(a component unit of the State of Illinois)**

**Schedule of Findings – State Compliance (Continued)
For the Two Years Ended June 30, 2023**

Prior Findings Not Repeated (Continued)

E. Lack of Agreement to Ensure Compliance with IT Security Requirements

During the previous examination, the State Employees' Retirement System of Illinois (System) had not entered into a detailed agreement with the Department of Innovation and Technology (DoIT) to ensure prescribed requirements and available security mechanisms were in place in order to protect the security, processing integrity, availability, and confidentiality of its systems and data.

During the current examination, our testing indicated the System used DoIT for limited services and was making improvements in reviewing internal controls for DoIT. (Finding Code No. 2021-006)