STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY

INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM

Report Required Under
Government Auditing Standards

For the Year Ended June 30, 2025

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

STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY
INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM
For the Year Ended June 30, 2025

TABLE OF CONTENTS

STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY
INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM
For the Year Ended June 30, 2025

DEPARTMENT OFFICIALS

Secretary (Acting) (3/21/25 - Present)	Mr. Brandon Ragle
Secretary (7/1/24 – 3/20/25)	Mr. Sanjay Gupta
Deputy Secretary (Acting) (6/16/25 – Present)	Mr. Patrick Nolan
Deputy Secretary (3/21/25 – 6/15/25)	Vacant
Deputy Secretary (7/1/24 – 3/20/25)	Mr. Brandon Ragle
Assistant Secretary (Acting) (5/16/25 – Present)	Mr. Christopher Britten
Assistant Secretary (7/1/24 – 5/15/25)	Vacant
Chief of Staff	Mrs. Jenifer Johnson
Chief Administrative Officer	Mr. Albert Coll
Chief Technology Officer	Mrs. Lori Sorenson
Chief Data Officer	Vacant
Chief Information Security Officer	Mr. Jason Bowen
Chief Enterprise Architect	Mr. William Downing
ERP Program Director (6/16/25 – Present)	Mrs. Kelly Turner
ERP Program Director (2/16/15 – 6/15/25)	Vacant
ERP Program Director (7/1/24 – 2/15/25)	Mrs. Tara Kessler
Chief Internal Auditor	Mr. John Valtierra
Affirmative Action/Equal Employment Opportunity Officer	Mrs. Vickie Simpson
Chief of Supplier Diversity	Mrs. Aliceber Rivera
Chief Information Accessibility Officer	Mr. Michael Scott
Chief Fiscal Officer	Mrs. Mary Feagans
General Counsel	Mrs. Radhika Lakhani

DEPARTMENT OFFICIALS - Continued

Group Chief Information Officers	
Health & Human Services	Mr. Stephen "Troy" Horton
Government & Public Employees	Mr. Sultan Raziuddin
Business & Workforce	Mrs. Lora McDonald
Natural & Cultural Resources	Mr. Andrew Martin
Public Safety (5/16/25 – Present)	Vacant
Public Safety (7/1/24 – 5/15/25)	Mr. Christopher Britten
Child & Family Services & Advocacy* (5/1/25 – Present)	Mrs. Rachel Pevey
Child & Family Services & Advocacy (2/1/25 – 4/30/25	Vacant
Education (1/1/25 – 1/31/25)	Vacant
Education (7/1/24 – 12/31/24)	Mrs. Mary Reynolds

*The Education group name changed to Child & Family Services & Advocacy effective 2/1/25.

DEPARTMENT OFFICES

The Department's primary administrative offices are located at:

120 W. Jefferson Street
Springfield, Illinois 62702-5170

201 W. Adams Street
Springfield, Illinois 62702-5170

GOVERNMENT AUDITING STANDARDS REPORT

SUMMARY

The examination of the "Management of the State of Illinois, Department of Innovation and Technology's Description of its Information Technology Shared Services System" (System and Organization Controls Report) was performed by Sikich CPA LLC in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

Based on their examination, the Service Auditors expressed a qualified opinion on the Department's "Management of the State of Illinois, Department of Innovation and Technology's Description of its Information Technology Shared Services System." The System and Organization Controls Report was issued under separate cover dated October 3, 2025.

SUMMARY OF FINDINGS

The Service Auditors identified certain deficiencies in internal control over the "Management of the State of Illinois, Department of Innovation and Technology's Description of its Information Technology Shared Services System" that are considered to be a material weakness.

SCHEDULE OF FINDINGS

Item No.	Page	Last/First Reported	Description	Finding Type
			Current Findings	
2025-001	7	2025/2025	Controls Were Not Suitably Designed or Did Not Operate Effectively	Material Weakness
			Prior Findings Not Repeated	
A	11	2024/2024	Controls Were Not Suitably Designed or Did Not Operate Effectively	Material Weakness

EXIT CONFERENCE

This report was discussed with Department personnel at an exit conference on September 30, 2025. Attending were:

Representing the Department of Innovation and Technology
Brandon Ragle, Acting Secretary
Pat Nolan, Deputy Secretary
Jenifer L. Johnson, Chief of Staff
John Valtierra, Chief Internal Auditor
Jason Barth, Chief Operating Officer
Markus Veile, Deputy Chief Information Security Officer
Lori Sorenson, Chief Technology Officer
William Roth, Chief of Enterprise Applications Services
Kelly Turner, ERP Program Director
Barbara Piwowarski, ERP Program Manager
Nana Mkheidze, Information System Internal Auditor
Dena Shelton, External Audit Coordinator
Radhika D. Lakhani, General Counsel

Office of the Auditor General
Reddy Bommareddi, Senior Audit Manager

Sikich CPA LLC
Amy L. Sherwood, Principal
Julie Schmidt, Director
Kirsten Orr, Director
Samantha Bugg, Senior Manager
Bridget Tolan, Manager
Zach Parker, Senior Technology and Risk Assessor

INDEPENDENT SERVICE AUDITOR'S REPORT ON INTERNAL CONTROL OVER REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN EXAMINATION OF A SERVICE ORGANIZATION PERFORMED IN ACCORDANCE WITH *GOVERNMENT AUDITING STANDARDS*

Honorable Frank J. Mautino
Auditor General
State of Illinois

As Special Assistant Auditors for the Auditor General, we have examined, in accordance with the attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the State of Illinois, Department of Innovation and Technology's (Department) "Management of the State of Illinois, Department of Innovation and Technology's Description of its Information Technology Shared Services System" (description) throughout the period from July 1, 2024, through June 30, 2025, and have issued our report thereon under a separate cover dated October 3, 2025. The report was modified due to certain matters related to internal control design and monitoring.

Report on Internal Control Over Reporting

Management of the Department is responsible for establishing and maintaining effective internal control over (1) fairly presenting the Department's description throughout the period from July 1, 2024, through June 30, 2025, and (2) establishing and maintaining effective internal control over the suitable design and operating effectiveness of the controls related to the control objectives within the Department's description throughout the period from July 1, 2024, through June 30, 2025.

In planning and performing our examination, we considered the Department's internal control as a basis for designing examination procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the Department's description throughout the period from July 1, 2024, through June 30, 2025, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Department's description 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 second paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. We identified certain deficiencies in internal control, described in the accompanying Schedule of Findings as item 2025-001 that we consider to be a material weakness.

Report on Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Department's description throughout the period from July 1, 2024, through June 30, 2025, is fairly presented and the controls related to the control objectives in the Department's description throughout the period from July 1, 2024, through June 30, 2025, were suitably designed and operating effectively, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the Department's description throughout the period from July 1, 2024, through June 30, 2025. However, providing an opinion on compliance with those provisions was not an objective of our examination and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards.*

Department's Response to the Finding

Government Auditing Standards requires the auditor to perform limited procedures on the Department's response to the finding identified in our examination and described in the accompanying Schedule of Findings. The Department's response was not subjected to the procedures applied in the examination and, accordingly, we express no opinion on the response.

Purpose of this Report

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

SIGNED ORIGINAL ON FILE

Springfield, Illinois
October 3, 2025

SCHEDULE OF FINDINGS

2025-001. **FINDING** (Controls Were Not Suitably Designed or Did Not Operate Effectively)

The controls related to the control objectives addressing system edits and validations, logical access, and physical access stated in the "Management of the State of Illinois, Department of Innovation and Technology's Description of its Information Technology Shared Services System" (description), provided by the Department of Innovation and Technology (Department), were not suitably designed or did not operate effectively to provide reasonable assurance the control objectives would be achieved.

During our testing, we noted the following controls were not suitably designed or did not operate effectively to provide reasonable assurance the control objective would be achieved:

System Edits and Validations

System edits and validations are mechanisms used within a system software to ensure the data entered into a system is accurate, complete, and conforms to expected formats or business rules. These rules are typically applied during data entry or data processing to verify the data meets criteria. They are critical for maintaining quality, integrity, and consistency by preventing incorrect or illogical data from being accepted into the system.

Department management was unable to provide a complete and reliable population of the Central Payroll System (CPS) and eTime system edits and validations used in its processing environment. Due to this condition, we were unable to conclude the Department's population records were sufficiently precise and detailed under the Attestation Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 320.30) to test the suitable design of the controls. Additionally, the edit check controls within CPS were not suitably designed. The CPS manual, which was ultimately used to derive a listing of screens and fields to sample, was outdated and inaccurate. Specifically:

- CPS –We noted one of nine (11%) screens documented in the manual was no longer in use and had not been maintained to reflect the current system configuration.

- eTime –The Department provided a manually maintained listing of system edits and validations. However, during testing we noted twenty of 37 (54%) edits and validations were defunct and had not been maintained to reflect the current system configuration.

Logical Access

Access controls are security measures used within systems to regulate who can access resources – such as data, applications, or system features – and what actions they can perform. Access controls help protect sensitive information, enforce privacy, and limit the potential for misuse or unauthorized activity within a system.

During testing, we noted the logical access controls were not operating effectively to ensure access to Department resources was authorized and approved. Specifically:

- Inappropriate User Access –
    - The Department was unable to provide evidence (system listing or access request form) to demonstrate authorized pre-approvals were obtained for the two of two (100%) users, who were provisioned access to merge eTime changes to production. To merge a change into production means to integrate finalized code or configuration updates into the live, customer-facing environment of a system or application.
    - We compared the population of developers to the population of users who can update the production environment and noted three users were granted conflicting access to both the development and production environment for the CPS application. This means the users can develop or modify code/configurations and directly deploy or update the production environment.
- Revocation of Access – Access was not revoked by the end of the next business day following the employee's or contractor's last day of work in accordance with Department procedures for two of 34 (6%) terminated users.
- Recertification of Access - Two user accounts requested to be revoked for one of 31 (3%) proxy agencies during the annual access review were not revoked.

Physical Access

Physical access controls are security measures designed to restrict or allow physical access to buildings, rooms, or physical IT assets like servers and workstations. Their main purpose is to protect people, property, and information from unauthorized physical intrusion, theft, damage, or harm.

During testing, we noted the physical access controls were not operating effectively to ensure physical access to Department facilities was restricted to authorized personnel. Specifically:

- Revocation of Access –For seven of 46 (15%) separated/terminated users, the Department could not provide completed badge access removal forms.

- Recertification of Access –

    - User access for individuals with access to the Central Computing Facility (CCF), Communications Building, and Warehouse was not verified during the first quarter of Fiscal Year 2025 access review in accordance with the Department policy.

    - User access for individuals with access to the CCF secured area was not verified for one of three (33%) monthly reviews.

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 Information Integrity (SI) section SI-10, requires entities to ensure systems validate input data for accuracy, completeness, and appropriateness utilizing system edits and validations to prevent erroneous or malicious data entry. Additionally, section SI-11 requires entities to ensure systems detect and handle errors securely and appropriately. The Access Control section AC-3 requires entities to develop and comply with the controls over the timely termination of access rights. The Configuration Management section CM-5 limits privileges to change system components within a production or operational environment. The Physical and Environmental Protection section PE-2 requires access authorizations to be revoked when an individual no longer requires access and calls for periodic reviews of access authorizations to ensure they remain appropriate.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the Department to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance that resources and 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.

Department officials indicated the exceptions occurred due to oversight, changes in team responsibility, and human error.

Failure to provide system edit and validation populations and ensure the operating effectiveness of logical and physical access controls resulted in a qualified opinion on the Department's System and Organization Controls Report. Additionally, without controls that are suitably designed and operating effectively at the Department, the user agencies' auditors will be unable to rely on the Department's controls relevant to the user agencies' internal control over financial reporting. (Finding Code No. 2025-001)

RECOMMENDATION

We recommend the Department ensure the controls are suitably designed and operating effectively over the services provided to user agencies, specifically involving system edits and validations and logical and physical access.

DEPARTMENT RESPONSE

The Department agrees with the recommendation. The Department will evaluate and strengthen its controls to ensure that system documentation is up to date, system access processes are refined, and physical access processes are streamlined with access reviews performed on schedule.

STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY
PRIOR YEAR FINDINGS NOT REPEATED
For the Year Ended June 30, 2025

A. **FINDING** (Controls Were Not Suitably Designed or Did Not Operate Effectively)

During the prior examination, the Department of Innovation and Technology (Department) did not ensure its controls over the State's Information Technology Shared Services System were suitably designed or operated effectively. Specifically, the Department was unable to provide populations related to unsuccessful backups and processing deviations, problems, and errors.

During the current examination, the Department provided such populations. (Finding Code No. 2024-001)