SIKICH



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, 2026

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, 2026

Table of Contents

	Page(s)
Department Officials	1-3
Summary	4-5
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*	6-7
Schedule of Findings	8-10

Department Officials

Secretary (5/13/26 – Present)	Brandon Ragle
Secretary (Acting) (7/1/25 – 5/12/26)	Brandon Ragle
Deputy Secretary (5/13/26 – Present)	Patrick Nolan
Deputy Secretary (Acting) (7/1/25 – 5/12/26)	Patrick Nolan
Assistant Secretary (5/13/26 – Present)	Christopher Britten
Assistant Secretary (Acting) (7/1/25 – 5/12/26)	Christopher Britten
Chief of Staff	Jenifer Johnson
Chief Operations Officer (9/1/25 – Present)	Jason Barth
Chief Operations Officer (8/15/25 – 8/31/25)*	Vacant
*Established and exempted 8/15/25	
Chief Administrative Officer	Albert Coll
Chief Technology Officer	Lori Sorenson
Chief Information Security Officer	Jason Bowen
Chief Internal Auditor	John Valtierra
Affirmative Action/Equal Employment Opportunity Officer	Vickie Simpson
Chief Fiscal Officer	Mary Feagans

Department Officials - Continued

General Counsel	Radhika Lakhani
Chief Information Accessibility Officer	Michael Scott
ERP Program Director	Kelly Turner
Chief Enterprise Architect	William Downing
Chief Data Officer (9/2/25 – Present)	Florence Castro-Wright
Chief Data Officer (7/1/25 – 9/1/25)	Vacant
Enterprise Project Management Executive	Sree Govindan Nair
Chief of Enterprise Application Services (11/16/25 – Present)	Bradley Smith
Chief of Enterprise Application Services (7/1/25 – 11/15/25)	William Roth
Chief Artificial Intelligence Officer (7/3/26 – Present)	Vacant
Chief Artificial Intelligence Officer (6/1/26 – 7/2/26)	Kader Sakkaria
Chief Artificial Intelligence Officer (11/21/25 – 5/31/26)*	Vacant

*Established and exempted 11/21/25

Group Chief Information Officers

Healthcare & Human Services	Stephen “Troy” Horton
Government & Public Employees	Sultan Raziuddin
Business & Workforce	Lora McDonald

Department Officials - Continued

Group Chief Information Officers - Continued

Natural & Cultural Resources (12/16/25 – Present)	David McKee
Natural & Cultural Resources (11/16/25 – 12/15/25)	Vacant
Natural & Cultural Resources (7/1/25 – 11/15/25)	Andrew Martin
Public Safety (7/16/25 – Present)	Cheryl Kulavic-Knope
Public Safety (7/1/25 – 7/15/25)	Vacant
Child & Family Services & Advocacy	Rachel Pevey

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 a separate cover dated October 14, 2026.

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	
2026-001	8	2026/2025	Controls Were Not Suitably Designed or Did Not Operate Effectively	Material Weakness
			Prior Findings Not Repeated	
None.				

Exit Conference

This report was discussed with Department personnel at an exit conference on October 6, 2026. Attending were:

Department of Innovation and Technology

Brandon Ragle, Secretary

Chris Britten, Assistant Secretary

Jenifer Johnson, Chief of Staff

John Valtierra, Chief Internal Auditor

Markus Veile, Deputy Chief Information Security Officer

Mary Feagans, Chief Fiscal Officer

Alexandra Albright, Chief Compliance Officer

Jason Bowen, Statewide Chief Information Security Officer

Brad Smith, Chief Enterprise Application Services

John Kennedy, EPMO Program Manager

Kelly Turner, ERP Program Director

Dena Shelton, External Audit Coordinator

Nana Mkheidze, IT Internal Auditor

Kristen Drainer, Internal Auditor

Radhika Lakhani, General Counsel

Office of the Auditor General

Reddy Bommareddi, Senior Audit Manager

Sikich CPA LLC

Amy Sherwood, Principal

Kirsten Orr, Director

Samantha Bugg, Senior Manager

Zach Parker, Manager

SIKICH®

Certified Public Accountants & Advisors
Members of American Institute of Certified Public Accountants

3051 Hollis Dr., 3rd Floor

Springfield, IL 62704

+1 (217) 793-3363

sikich.com

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 Christopher B. Meister
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, 2025, through June 30, 2026, and have issued our report thereon under a separate cover dated October 14, 2026. The report was modified due to certain matters related to suitability of design and operating effectiveness of controls.

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, 2025, through June 30, 2026, 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, 2025, through June 30, 2026.

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, 2025, through June 30, 2026, 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 2026-001 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, 2025, through June 30, 2026, is fairly presented and the controls related to the control objectives in the Department's description throughout the period from July 1, 2025, through June 30, 2026, 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, 2025, through June 30, 2026. 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 14, 2026

Schedule of Findings

2026-001 **FINDING** (Controls were not suitably designed or did not operate effectively)

The controls related to the control objectives addressing system processing and error handling, change management, physical access, and logical 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 processing and error handling

System processing and error handling procedures ensure system errors and processing exceptions are identified, documented, investigated, and resolved in a timely manner. Effective monitoring and resolution of technical abends—abnormal terminations of an application, program, or system process caused by processing errors or system conditions—support the reliability and integrity of system data by providing assurance that processing issues are appropriately addressed.

During testing, we noted the Department has not designed and implemented a formalized process to document and monitor abends to resolution.

Change management

Change management controls are processes and procedures designed to ensure changes to information systems are appropriately authorized, tested, approved, documented, and implemented. Their primary purpose is to reduce the risk of service disruptions, security vulnerabilities, or other unintended consequences resulting from changes to production systems.

During testing, we noted change management controls were not operating effectively to ensure system changes were implemented in accordance with established Department procedures. Specifically, systems were not patched during one of three (33%) months tested.

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:

- Background check – For two of 24 (8%) individuals tested, the Department could not provide evidence of the required attestation of a clear background check completed within the five years preceding badge issuance.

- 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 2026 access review in accordance with the Department's policy.

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

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:

- 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 three of 37 (8%) separated users tested. Access was revoked three to 46 days late.

- Provisioning of Access – Access was inadvertently provisioned to the wrong user for one of 33 (3%) access requests tested.

- Weekly Access Violation Report Reviews – The Department was unable to provide evidence that weekly access violation reports were produced and reviewed in accordance with established procedures for two of seven (29%) weeks tested.

In the 2025 examination, we noted that the Department could not provide a complete and reliable population of Central Payroll System (CPS) and eTime system edits and validations used in its processing environment. In the current examination, the Department provided such populations. Additionally, the prior year exceptions regarding documentation of privileged access approvals, conflicting developer and production system access, removal of access identified during annual recertification reviews, and documentation of completed badge access removal forms were not repeated during the current examination period.

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-2 requires entities to identify and correct system flaws and install security-related patches within a defined timeframe.

Additionally, SI-11 requires entities to ensure systems detect and handle errors securely and appropriately. The Access Control (AC) section AC-2 requires entities to manage information system accounts, including establishing conditions for group and role membership and assigning access based on approved authorizations. Additionally, section AC-3 requires entities to develop and comply with the controls over the timely termination of access rights. The Personnel Security (PS) section PS-3 requires entities to conduct personnel screening and rescreening activities in accordance with applicable laws, regulations, policies, standards, and risk designations associated with assigned positions. The PS-3 section also requires organizations to establish criteria and frequencies for screening individuals with access to systems and information and may include background investigations and agency checks. The Physical and Environmental Protection (PE) 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 implementation of new processes and human error.

Failure to design and implement a formalized process to document and monitor system abends to resolution and ensure the operating effectiveness of change management, logical access, 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. 2026-001, 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 processing and error handling, change management, and physical and logical access.

DEPARTMENT RESPONSE

The Department agrees with the recommendation. The Department will evaluate and strengthen its controls to ensure that procedures are established and followed to (1) document and monitor abends to resolution, (2) provision, monitor, and revoke physical and logical access, and (3) implement change management controls.