STATE OF ILLINOIS
OFFICE OF THE
AUDITOR GENERAL
Frank J. Mautino, Auditor General

SUMMARY REPORT DIGEST

DEPARTMENT OF INNOVATION AND TECHNOLOGY
INFORMATION TECHNOLOGY HOSTING SERVICES

System and Organization Control Report and Report Required Under *Government Auditing Standards*
For the Year Ended June 30, 2022

Release Date: August 11, 2022

FINDINGS THIS AUDIT: 3

	New	Repeat	Total
Category 1:	**2**	**1**	**3**
Category 2:	**0**	**0**	**0**
Category 3:	**0**	**0**	**0**
TOTAL	**2**	**1**	**3**

FINDINGS LAST AUDIT: 1

AGING SCHEDULE OF REPEATED FINDINGS

Repeated Since	Category 1	Category 2	Category 3
2021	**22-3**		

INTRODUCTION

This digest covers the System and Organization Control Report and the Report Required under *Governmental Auditing Standards* of the Department of Innovation and Technology (Department) for the period of July 1, 2021 to June 30, 2022.

The System and Organization Control Report contained an adverse opinion due to weaknesses associated with the Department's Description of System, suitability of the control design and the operating effectiveness of controls. In addition, the Report Required under *Government Auditing Standards* (GAS) contains 3 findings.

SYNOPSIS

- (**22-1**) The "Description of the State of Illinois, Information Technology Hosting Services" contained inaccuracies and omissions.
- (**22-2**) The controls related to the trust services criteria stated in the "Description of the State of Illinois, Information Technology Hosting Services" were not suitably designed to provide reasonable assurance the trust services criteria would be achieved.
- (**22-3**) The controls related to the trust services criteria stated in the "Description of the State of Illinois, Information Technology Hosting Services" did not operate effectively.

Category 1: Findings that are **material weaknesses** in internal control and/or a **qualification** on compliance with State laws and regulations (material noncompliance).

Category 2: Findings that are **significant deficiencies** in internal control and **noncompliance** with State laws and regulations.

Category 3: Findings that have **no internal control issues but are in noncompliance** with State laws and regulations.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

INACCURATE DESCRIPTION OF SYSTEM

Inaccurate description of system

The “Description of the State of Illinois, Information Technology Hosting Services” (description of system), as provided by the Department of Innovation and Technology (Department), contained inaccuracies and omissions.

During our examination of the Department’s description of system, we noted it contained inaccuracies. Specifically, we noted:

Inaccurate statements

Control stated in the description of system	Actual control in place
The Department conducts risk assessments for customer agencies.	The Department was to conduct risk assessments for all agencies, boards, and commissions under the Governor.
In the event of an emergency, only verbal approval by the appropriate management personnel is required to begin remediation.	The emergency Change Advisory Board (eCAB) approval is required in order for remediation actions to begin.

Omitted internal control

In addition, our examination noted the Department’s description of system did not document the Department’s recovery activities associated with the midrange environment. (Finding 1, pages 8-9 of GAS Report)

We recommended the Department review the description of system to ensure it accurately depicts all internal controls over the services provided to user agencies.

Department agreed

Department officials agreed and stated they would review the description of system and make any necessary changes as needed.

CONTROLS WERE NOT SUITABLY DESIGNED

Controls not suitably designed

The controls related to the trust services criteria stated in the “Description of the State of Illinois, Information Technology Hosting Services” (description of system), as provided by the Department of Innovation and Technology (Department), were not suitably designed to provide reasonable assurance the trust services criteria would be achieved.

Inadequate policies and procedures

During our testing we noted the Department’s Change Management Guide and the Change Management Process did not document:

- The change prioritization requirements;

- Required fields to be completed for each type of change;
- Documentation requirements for Post Implementation Reviews;
- Documentation requirements for testing, implementation and backout plans; and
- The approval process in place.

Internal controls not documented

In addition, the Department had not documented the internal controls regarding access provisioning of staff and vendors to gain access to network devices. Further, the Department had not documented the internal controls over modification and revocation of mainframe access.

As a result, we were unable to determine if the controls were suitably designed. (Finding 2, pages 10-11 of GAS Report)

We recommended the Department ensure the controls are suitably designed over the services provided to user agencies.

Department agreed

Department officials agreed and stated they would review the controls in place to ensure they are effectively designed.

CONTROLS DID NOT OPERATE EFFECTIVELY

Controls did not operate effectively

The controls related to the trust services criteria stated in the "Description of the State of Illinois, Information Technology Hosting Services" (description of system), provided by the Department of Innovation and Technology (Department), did not operate effectively.

Populations not provided

As part of our testing to determine if the controls were operating effectively, we requested the Department provide populations related to:

- Risk assessments completed;
- New administrator logical access request for access;
- Active Directory access modifications;
- Security Software accounts created;
- Lost or stolen laptops;
- Physical access request for non-State employees;
- Incident tickets; and
- Changes made to applications and the environment, including emergency changes.

However, the Department did not provide complete and accurate populations.

In addition, the Department provided a report regarding the Security Awareness Training completed during the examination period; however, we determine the report to be incomplete.

Testing could not be performed

As such, we could not perform testing.

Additionally, during our testing of the controls related to the trust services criteria stated in the description of system; however, we noted specific controls which did not operate effectively. Specifically, we noted:

Did not ensure compliance with Policies

Compliance with Policies

- The Department did not ensure the Department's compliance with all of the enterprise information security policies.

Human Resource weaknesses

Human Resources

- The specified required background checks were not always completed.
- Employees and contractors did not always complete the required training within 30 days of hiring.
- Employees did not always complete the annual Ethics Training Program for State of Illinois Employees and Appointees and the Information Safeguard training.
- Annual and probationary evaluations were not always completed or completed timely.

Subservice providers' weaknesses

Subservice Providers

- Subservice providers' contracts did not always contain the requirement for the subservice provider to contact the Department in the event of a security incident or information breach.
- Meetings between the Department and the service providers were not conducted in accordance to the documented schedule.

Change management policies not followed

Change Management

- The Endpoint Protection Group did not follow the Department's Change Management Process.

Logical security weaknesses

Logical Security

- Documentation demonstrating separated employees' and contractors' midrange logical access was revoked was not provided for all of the instances selected.
- Separated employees and contractors did not always have their midrange logical access revoked on their last working day.
- Documentation demonstrating access with powerful privileges, high-level access and access to sensitive system functions was restricted to authorized personnel was not provided.
- Documentation demonstrating separated employees' and contractors' mainframe accounts had been revoked was not provided for all of the instances selected.
- Security settings did not conform to the Department's or vendor's standards.
- New requests for access to the Department's midrange resources were not always properly approved.

- Service requests or Exit forms were not always completed for separated employees and contractors.
- Guidance was not provided to the agencies related to the remediation of identified vulnerabilities.

Physical security weaknesses

Physical Security

- Physical security controls were not always properly implemented.
- Documentation demonstrating separated or terminated individuals' physical access had been deactivated was not provided.
- New employees' and contractors' badge request forms were not always properly completed or did not contain documentation of proof of identity.
- New employees' and contractors' access to the data center's secured location was not always approved.
- Individuals were issued temporary badges with inappropriate access to the Department's buildings.
- The Building Admittance Registers were not always maintained.

Security violation weaknesses

Security Violations

- The Incident Management Response Process Guide had not been updated to reflect the transition of service management tools and processes.
- Thresholds had not been established to determine which violations were followed up on.
- Mainframe monitoring reports were not always completed and distributed monthly.
- Security incidents did not always contain notification to the agency, documentation the Executive Summary or Incident Report was provided to the affected agency, and status updates.

Backup weaknesses

Backups

- Documentation demonstrating the replication between the Department's data center and alternate data center occurred and the Enterprise Storage and Backup group received an alert if the data was out of sync for defined period of time was not provided.
- Midrange server backup reports were not provided for all of the instances selected.

Disaster recovery weaknesses

Disaster Recovery

- Several mainframe critical applications tested were aborted before user testing was completed. (Finding 3, pages 12-14 of GAS Report)

We recommended the Department ensure its controls operate effectively over the services provided to user agencies.

Department agreed

Department officials agreed and stated they would review the control in place to ensure they are operating effectively.

DEPARTMENT’S SECRETARY

During the examination period:
Jennifer Ricker (4/9/22 – present)
Jennifer Ricker, Acting (7/1/21 – 4/8/22)

SERVICE AUDITOR’S OPINION

The System and Organization Control Report contained an adverse opinion. Specifically, the Service Auditors determined:

a. the description does not present the system that was designed and implemented throughout the period July 1, 2021 to June 30, 2022 in accordance with the description criteria.

b. the controls stated in the description were not suitably designed throughout the period July 1, 2021 to June 30, 2022 to provide reasonable assurance that the Department’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c. the controls stated in the description did not operate effectively throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that the Department’s service commitments and system requirements were achieved based on the applicable trust services criteria.

This System and Organization Control Examination was conducted by the Office of the Auditor General’s staff.

SIGNED ORIGINAL ON FILE

JANE CLARK
Division Director

This report is transmitted in accordance with Section 3-14 of the Illinois State Auditing Act .

SIGNED ORIGINAL ON FILE

FRANK J. MAUTINO
Auditor General

FJM:mkl