



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, 2023

Release Date: September 7, 2023

FINDINGS THIS AUDIT: 2	AGING SCHEDULE OF REPEATED FINDINGS						
	New	Repeat	Total	Repeated Since	Category 1	Category 2	Category 3
Category 1:	0	2	2	2022	23-1		
Category 2:	0	0	0	2021	23-2		
Category 3:	0	0	0				
TOTAL	0	2	2				
FINDINGS LAST AUDIT: 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, 2022 to June 30, 2023.

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 two findings.

SYNOPSIS

- (23-1) 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.
- (23-2) 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**

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.

Complete and accurate populations not provided

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

- New hires and Personal Service Contractors.
- Risk assessments completed.
- New Agency Application Administrator logical access requests;
- Active Directory access requests, modifications and terminations;
- Security Software accounts created, modified, and revoked;
- New Security Software Administrator accounts;
- New and terminated physical access request, including non-State employees;
- Major outage incidents; and
- Changes made to applications.

Testing not performed

However, the Department did not provide complete and accurate populations. As such we could not perform testing.

Department did not respond to request

The Department did not provide a complete and accurate report demonstrating employees and Personal Service Contractors had completed Security Awareness Training and Information Safeguarding Training. In addition, the Department did not respond to our request regarding staff and vendors with a business need to access or modify network devices.

Change management procedures and process not followed

Our testing also noted the Department did not follow their change management procedures or processes for changes to the mainframe operating system and the network security tool. Lastly, the Department was unable to demonstrate they were monitoring for compliance with the enterprise information security policies.

As a result, we were unable to determine if the controls were suitably designed. (Finding 1, pages 8-9 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 and would work 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.

During our testing of the controls related to the control objectives stated in the description of system, we noted specific controls which did not operate effectively. Specifically, we noted:

Human Resource

Human Resource weaknesses

- Performance evaluations were not provided to the auditors or were not always completed.

Change Management

Change management weaknesses

- Post Implementation Reviews were not always completed timely.
- Some changes did not have a test plan.
- Changes to the environment operating systems were not always approved.

Physical Security

Physical security weaknesses

- A monthly review of the Central Computing Facility (CCF) secured area was not completed.
- Individuals were issued temporary badges with inappropriate access to the Department’s buildings.

Logical Security

Logical security weaknesses

- Security software weekly violation reports did not document if violations were followed up on or reviewed.
- The Department did not provide several proxy agencies a listing of their security software accounts for review.
- Security settings did not always conform to the Department’s or vendor’s standards. The IT Service Desk emailed the security software account temporary password, instead of contacting the individual.
- Some lost or stolen devices did not have verification conducted to determine if encryption was installed.

Security Violations

Security violation weaknesses

- Security violation reports did not document followup actions taken related to security violations.
- Mainframe monitoring reports were not always completed and distributed.

- Some security incidents did not document the agency was notified or the Executive Summary or Incident Report was provided.

Policies and procedures not updated

Environments

- Several policies and procedures had not been updated to reflect current processes.

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 an incident or information breach.
- A subservice provider’s contract did not cover the entire examination period.
- Meetings between the Department and the subservice providers were not conducted in accordance with the documented schedule.
- System and Organization Control Reports and bridge letters were not always obtained documenting the subservice providers’ internal controls extended throughout the examination period. (Finding 2, page 10-11 of GAS Report) This finding has repeated since 2021

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 controls in place and would work to ensure they are operating effectively.

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, 2022 to June 30, 2023 in accordance with the description criteria.
- b. the controls stated in the description were not suitably designed throughout the period July 1, 2022 to June 30, 2023 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, 2022 to June 30, 2023, 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