



STATE OF ILLINOIS
**OFFICE OF THE
 AUDITOR GENERAL**

Frank J. Mautino, Auditor General

SUMMARY REPORT DIGEST

**DEPARTMENT OF INNOVATION AND TECHNOLOGY
INFORMATION TECHNOLOGY SHARED SERVICES**

System and Organization Control Report and Report
 Required Under *Government Auditing Standards*
 For the Year Ended June 30, 2020

Release Date: August 12, 2020

FINDINGS THIS AUDIT: 2				AGING SCHEDULE OF REPEATED FINDINGS			
	<u>New</u>	<u>Repeat</u>	<u>Total</u>	<u>Repeated Since</u>	<u>Category 1</u>	<u>Category 2</u>	<u>Category 3</u>
Category 1:	0	2	2	2018	1, 2		
Category 2:	0	0	0				
Category 3:	<u>0</u>	<u>0</u>	<u>0</u>				
TOTAL	0	2	2				
FINDINGS LAST AUDIT: 3							

INTRODUCTION

This digest covers our System and Organization Control Report and Report Required Under *Government Auditing Standards* of the Department of Innovation and Technology (Department) Information Technology Shared Services for the period from July 1, 2019 through June 30, 2020.

The Department provides information technology general controls and application controls for approximately 105 user agencies.

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

SYNOPSIS

- **(20-1)** The Department did not ensure all its controls were suitably designed to achieve its control objectives.
- **(20-2)** The Department did not ensure its controls over the State's Shared Services system operated 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 were not suitably designed	The Department of Innovation and Technology (Department) did not ensure all its controls were suitably designed to achieve its control objectives. The controls related to the control objectives are stated in the “Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls” (description of system), provided by the Department.
Access controls did not operate for a period of time	<p>The Department stated in its description of system that controls were not in place for:</p> <ul style="list-style-type: none">• Access reviews to the Communication Building during the period of July 1, 2019, to December 31, 2019; and,• Access reviews to the Department’s Central Computing Facility highly secured area during the period of July 1, 2019, to November 30, 2019. <p>As a result of the above noted exceptions, the controls were not suitably designed. (Finding 1, page 8 of GAS Report)</p> <p>We recommended the Department ensure the controls are suitably designed over the services provided to user entities.</p>
Department agreed with Service Auditors	Department officials accepted the recommendation.

CONTROLS DID NOT OPERATE EFFECTIVELY

Controls did not operate effectively	The Department of Innovation and Technology (Department) did not ensure its controls over the State’s Shared Services system operated effectively. The controls related to the control objectives are stated in the “Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls” (description of system), provided by the Department.
Population was not available to conduct tests of controls	As part of our testing to determine if the controls were operating effectively, we requested the Department to provide a population of modifications to employees’ and contractors’ access to the Department’s resources. However, the Department was unable to provide a population. As a result of the Department’s inability to provide the population, we were unable to conduct testing to determine if the controls related to logical access to applications, data, and the environment were restricted to authorized and appropriate users.
Unable to verify completeness and accuracy of a population	Additionally, we requested the Department provide a population of an operating system’s patches applied during the examination period. Although the Department provided a population, they did not provide documentation demonstrating

the population was complete and accurate. Due to these conditions, we were unable to conclude the Department's population was sufficiently precise and detailed under the Attestation Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 320.30) to test the operating effectiveness of the control.

Furthermore, 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:

Logical access provisioning and de-provisioning weaknesses

- The Department was unable to provide documentation demonstrating the timely termination of individuals' access to the Department's resources.
- New employee and contractor access requests were not submitted by an authorized Agency Technology Service Requester or Department IT Coordinator.
- A new employee did not have an access request submitted to obtain access to the Department's resources.
- The annual technical account review controls did not include a defined timeframe for the disabling/deletion of accounts in the event a manager did not respond to the review request.

Physical access provisioning and de-provisioning weaknesses

- The Department was unable to provide a listing of individuals authorized to approve the DoIT Badge Request form.
- The Department was unable to provide documentation demonstrating terminated individuals' access badge was deactivated.
- Multiple instances where individuals were not properly authorized or should not have had access to one of the Department's facilities.
- An individual did not have a completed DoIT Badge Request form in order to obtain access to the Department's facilities.
- The Physical Access Door Group Review Procedures did not document the review frequency and the door groups which were to be reviewed.

Human resource weaknesses

- Multiple instances where employees or contractors:
 - did not have evaluations completed within the defined timeline.
 - did not complete the Safeguard Disclosure training and Security Awareness training.
 - did not have a completed Remedy service request for terminated employees.

Application edits weakness

- One state's tax rate was incorrect in the Central Payroll System tax tables.

Change management weaknesses

- The Change Management Process Guide did not contain information on the change freeze process.
- Changes did not always have test plans, backout plans, or implementation plans.
- Emergency changes did not always have a Post Implementation Review conducted.
- An emergency change was created and approved by the same individual; thus, creating a segregation of duties weakness.
- Changes were improperly categorized.

Help desk weakness

- Multiple instances where stolen or missing laptops did not have a verification completed to determine if encryption was installed.

Monitoring weaknesses

- A daily Resource Management Facility Report was not provided.
- Multiple threats did not have a documented incident report.
- Multiple threat incident reports were missing required segments: lessons learned, prevention recommendations, notifications, status updates, and an executive summary.

Device configurations weaknesses

- Multiple instances where:
 - Systems were not up-to-date with the latest anti-virus software.
 - Systems were not up-to-date with the latest virus definitions.
 - Systems did not have the anti-virus product version installed.
- Multiple instances where operating system patches were not tested prior to being pushed to the general populations.

Failure to ensure controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved resulted in a modified opinion on the Department's System and Organization Control Report related to the Information Technology Shared Services. (Finding 2, pages 9-11 of GAS Report)

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

Department agreed with Service Auditors

Department officials accepted the recommendation.

DEPARTMENT SECRETARY

During Examination Period:
Ron Guerrier (2/18/20 – Current)
Ron Guerrier, Acting (7/1/19 – 2/17/20)

SERVICE AUDITOR'S OPINION

The System and Organization Control Report contained a modified opinion. Specifically, the Service Auditors determined, except for the matters described in the System and Organization Control Report, in all material respects, based on the criteria described in the State of Illinois, Department of Innovation and Technology's assertion:

- the description fairly presents the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services system that was designed and implemented throughout the period from July 1, 2019 to June 30, 2020.
- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period from July 1, 2019, to June 30, 2020; and subservice organizations and user entities applied complementary controls assumed in the design of the State of Illinois, Department of Innovation and Technology's control throughout the period July 1, 2019 to June 30, 2020.
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period from July 1, 2019 to June 30, 2020 if complementary subservice organization and user entity controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls operated effectively throughout the period July 1, 2019 to June 30, 2020.

This System and Organization 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