## SUMMARY REPORT DIGEST

# DEPARTENT OF INNOVATION AND TECHNOLOGY
# INFORMATION TECHNOLOGY SHARED SERVICES

**System and Organization Control Report and Report**                    **Release Date:  August 11, 2022**
**Required Under** *Government Auditing Standards*
  **For the Year Ended June 30, 2022**

| FINDINGS THIS AUDIT: 3 | | | | AGING SCHEDULE OF REPEATED FINDINGS | | | |
|---|---|---|---|---|---|---|---|
| | New | Repeat | Total | Repeated Since | Category 1 | Category 2 | Category 3 |
| **Category 1:** | 2 | 1 | 3 | 2018 | 22-3 | | |
| **Category 2:** | 0 | 0 | 0 | | | | |
| **Category 3:** | 0 | 0 | 0 | | | | |
| **TOTAL** | 2 | 1 | 3 | | | | |
| **FINDINGS LAST AUDIT: 1** | | | | | | | |

## INTRODUCTION

This digest covers our System and Organization Control Report and Report Required under Government Auditing Standards of the Department of Innovation and Technology Information Technology Shared Services for the period from July 1, 2021 through June 30, 2022.

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

## SYNOPSIS

- (**22-1**)    The Description of the Information Technology Shared Services System for the Information Technology General Controls and Application Controls contained inaccuracies.

- (**22-2**)    The controls related to the control objectives stated in the Description of the Information Technology Shared Services System for the Information Technology General Controls and Application Controls were not suitably designed to provide reasonable assurance the control objectives would be achieved.

- (**22-3**)    The controls related to the control objectives stated in the Description of the Information Technology Shared Services System for the Information Technology General Controls and Application Controls 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 Information Technology Shared Services System for the Information Technology General Controls and Application Controls" (description of system), as provided by the Department of Innovation and Technology (Department), contained inaccuracies.

**Inaccurate statements**

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

| 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. |
| The Department's Division of Information Security is responsible for ensuring Department's compliance with enterprise information security policies. | The Department was to not ensuring the Department's compliance with all of the enterprise information security policies. |
| 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. |

(Finding 1, page 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 control objectives stated in the "Description of the Information Technology Shared Services System for the Information Technology General Controls and Application Controls" (description of system), provided by the Department of Innovation and Technology (Department), were not suitably designed to provide reasonable assurance the control objectives would be achieved.

**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 administrator logical access requests;
- Active Directory access modifications;
- Security Software accounts created, modified, and revoked;
- Agency Application Administrator changes;
- Changes to an antivirus tool;
- Physical access requests for non-State employees; and
- Changes made to applications and the environment, including emergency changes.

**Testing could not be performed**

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

**Inadequate policies and procedures**

In addition, 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.

Furthermore, the Application Lifecycle Management Manual did not document the responsibilities of the Change Management Team and the Change Advisory Board.

We also noted the Department did not document the access provisioning requirements in order for staff and vendors to gain access to network devices.

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 control objectives stated in the "Description of the Information Technology Shared Services System for the Information Technology General Controls and Application Controls" (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:

Change Management

**Change management weaknesses**

- Mainframe application changes were not always properly authorized prior to moving to the code management system.
- Mainframe application changes were not always approved prior to releasing to Library Services.
- eTime changes were not properly approved prior to deploying to the production environment.
- The Endpoint Protection Group did not follow the Department's Change Management Process.

Logical Security

**Logical security weaknesses**

- 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 always conform to the Department or vendor's standards.
- New requests for access to the Department's resources were not always properly approved.
- Service requests or Exit forms were not always completed for separated employees and contractors.

Physical Security

**Physical security weaknesses**

- Physical security controls were not always properly implemented.
- Documentation demonstrating separated or terminated individuals' physical access had been deactivated was not provided.
- New employee and contractor 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
- Thresholds had not been established to determine which violations were followed up on.
- Mainframe monitoring reports were not always completed and distributed monthly.

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 a defined period of time was not provided.
- Midrange server backup reports were not provided for all of the instances selected.
- Remediation efforts for specific midrange backups were not documented. (Finding 3, pages 12-13 of GAS Report)

**Backup weaknesses**

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 fairly presents the State of Illinois, Department of Innovation and Technology's Information Shared Services system that was designed and implemented throughout the period from July 1, 2021 to June 30, 2022.

b. the controls related to the control objectives stated in the description were not suitably designed to provide reasonable assurance that the control objectives would be achieved if the control operated effectively throughout the period July 1, 2021 to June 30, 2022.

c. the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, did not operate effectively throughout the period from July 1, 2021 to June 30, 2022.

The 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