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

SUMMARY REPORT DIGEST

DEPARTMENT OF INNOVATION AND TECHNOLOGY

System and Organization Control Report and Report Required Under *Government Auditing Standards*
For the Year Ended June 30, 2019

Release Date: August 14, 2019

FINDINGS THIS AUDIT: 3

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

FINDINGS LAST AUDIT: 3

AGING SCHEDULE OF REPEATED FINDINGS

Repeated Since	Category 1	Category 2	Category 3
2018	**1, 2, 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) for the period from July 1, 2018 through June 30, 2019.

The Department provides information technology general controls and application controls for approximately 101 user agencies.

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

SYNOPSIS

- **(19-1)** The Department's description of system contained inaccuracies and omissions.
- **(19-2)** The Department's controls stated in its description of system were not suitably designed to provide reasonable assurance that the control objectives would be achieved.
- **(19-3)** The Department's controls stated in its description of system were not operating 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

Inaccuracies and omissions in its description of system

The Department of Innovation and Technology's "Description of the IT General Controls and Application Controls for the Department of Innovation and Technology's Information Technology Shared Services System" (description of system) contained inaccuracies and omissions.

The Department provides State agencies with information technology general controls and application controls for their use. As such, the Department, as a service provider, provides services which are likely relevant to user agencies' internal control over financial reporting. Therefore, the Department is required to develop an accurate and complete description of system documenting their internal controls over the services provided.

Description of system had inaccurate statements

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

- Technical accounts were not reviewed annually;
- The ERP Production Support did not communicate through a dedicated email address;
- The Illinois Tollway did not go live with the ERP on July 1, 2017;
- The Incident Management Process Guide did not reflect the changes in the Major Outage Response Team (MORT) process;
- The Department did not publish the monthly, quarterly, or annual metric of incident statistics or provide to management;
- The Lost or Stolen Equipment Policy did not reflect the actual processes followed;
- Services and performance statistics were not communicated at the DoIT Daily meeting until September 12, 2018, and were never communicated at the CIO meetings;
- Antivirus definition files were not pushed out to servers beginning eight hours after availability;
- The System Management Facility violation record reports were not reviewed by the Manager of Mainframe Support Services;
- The Department was not responsible for the scheduling and backup of agencies' applications and data;
- The Department did not utilize Secure File Transfer Protocol (SFTP) to secure the transfer of mainframe data;

- The Department did not utilize security experts and vendor subscription services to assist in determining risk from potential and newly discovered vulnerabilities; and,
- Vulnerability scans were not conducted within the defined frequencies.

Description of system had omissions of internal controls

During our examination of the Department's description of system, we noted it contained omission of internal controls. Specific omissions included:

- complementary subservice organization controls for the subservice providers utilized;
- controls to comply with Complementary User Entities Controls documented in subservice providers' System and Organization Reports;
- controls for monitoring services provided by the Department of Central Management Services;
- controls over the maintenance and patching of the mainframe operating systems;
- the frequency for which backups were missed prior to the SQL Team being notified; and,
- a statement describing how the System Administrator ran the systems programmer and high profile user ID report and provided to the Manager of Mainframe Support Services. (Finding 1, pages 7-8 of GAS Report)

We recommended the Department review the description of system to ensure it is complete, accurate, and contains all internal controls over the services provided to user agencies.

Department agreed with Service Auditors

Department officials accepted the recommendation.

CONTROLS WERE NOT SUITABLY DESIGNED

Controls were not suitably designed

The Department of Innovation and Technology's controls related to the control objectives stated in the "Description of the IT General Controls and Application Controls for the Department of Innovation and Technology's Information Technology Shared Services system" (description of system) were not suitably designed to provide reasonable assurance that the control objectives would be achieved.

Populations were not available to conduct tests of controls

As part of testing to determine if the controls were suitably designed, we requested the Department to provide populations related to individuals authorized to approve physical access to Department facilities, change requests, and unplanned outages. However, the Department did not provide complete and accurate populations. As such, we were unable to conduct testing to determine if the controls were suitably designed.

In addition, during our testing, we noted:

- The Mainframe Change Management Procedures did not address the prioritization of requests, required approvals, testing and documentation requirements, and post implementation reviews;

- The WebServices Change Management Procedures did not address the prioritization of requests, required approvals, testing and documentation requirements, and post implementation reviews;
- Major Outage Response Team (MORT) incidents which occurred after business hours did not follow the documented process; and,
- The Department could not provide the Chief Information Officer's review of Incident Reports for the period from July 1, 2018 through March 31, 2019.

As a result of the above noted exceptions, we were unable to determine if the controls were suitably designed. (Finding 2, pages 9-10 of GAS Report)

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

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's controls related to the control objectives stated in the "Description of the IT General Controls and Application Controls for the Department of Innovation and Technology's Information Technology Shared Services System" (description of system) 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 Resources weaknesses

- Multiple instances where employees or contractors:
  - did not have properly completed DoIT Badge Request forms;
  - had not completed security awareness training or cybersecurity training;
  - did not have a probationary or annual evaluation completed or it was completed late; and,
  - had not completed the annual acknowledgement of compliance with security policies.

Access provisioning and de-provisioning weaknesses

- Instances occurred where:
  - Security software violation reports were not reviewed;
  - Separation reports were not reviewed;
  - Mainframe administrator accounts were not revoked;

  - Terminated individuals’ access was not revoked;
  - Terminated individuals’ access was not timely revoked; and,
  - HANA access requests were not completed.

Application Edits weaknesses

- 4 States’ tax rates were incorrect in the CPS tax tables.

Change Management weaknesses

- Changes related to applications and the infrastructure did not always have Backout Plans or Test Plans; and,
- ERP change request forms did not always have all required fields completed.

Device Configuration weaknesses

- Multiple instances where:
  - Systems were not up-to-date with the latest antivirus;
  - Systems were not up-to-date with the latest virus definitions;
  - Systems did not have antivirus product version installed; and,
  - The Department did not provide support demonstrating network hardware and software alerts were reviewed.

As a result of the above noted exceptions, the controls were not operating effectively to provide reasonable assurance that the control objectives stated in the description were achieved. (Finding 3, pages 11-12 of GAS Report)

Department agreed with Service Auditors

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

Department officials accepted the recommendation.

DEPARTMENT SECRETARY

During Examination Period:
Ron Guerrier, Acting (3/4/19 - Current)
Jennifer Ricker, Acting (2/11/19 - 3/3/19)
Jack King, Interim (1/1/19 - 2/11/19)
Kirk Lonbom, Acting (7/1/18 - 12/31/18)

SERVICE AUDITOR’S OPINION

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

- the description does not fairly present the description of system.

- the controls stated in the description of system were not suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated.

- the controls did not operate effectively to provide reasonable assurance that the control objectives stated in the description of system were achieved.

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