SUMMARY REPORT DIGEST

DEPARTMENT OF INNOVATION & TECHNOLOGY

Service Organization Control Report and Report Required Under *Government Auditing Standards*
  For the Year Ended June 30, 2018

Release Date: August 15, 2018

FINDINGS THIS AUDIT: 3			
	New	Repeat	Total
Category 1:	**3**	**0**	**3**
Category 2:	**0**	**0**	**0**
Category 3:	0	0	0
TOTAL	**3**	**0**	**3**

INTRODUCTION

This digest covers our Service Organization Control Report and Report Required Under *Government Auditing Standards* of the Department of Innovation & Technology (Department) for the period of July 1, 2017 to June 30, 2018.

The Department provides information technology general controls and application controls for approximately 103 user agencies.

The Service 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 3 findings.

SYNOPSIS

- **(18-1)** The Department's Description of System contained inaccuracies and omissions.

- **(18-2)** 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.

- **(18-3)** 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 & Technology's (Department) "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services System" (Description of System) contained inaccuracies and omissions.

Department provides IT services to 103 user agencies

The Department provides State agencies 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:
- The IT Risk Assessment Policy was no longer utilized by the Department.
- Ethics training and the DCMS Policy Manual were not provided to newly hired contractors.
- Developers did not obtain user acceptance approvals over changes to Common Systems.

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 they utilized.
- Information regarding the configuration standards and installation requirements for midrange devices.
- Information on the secondary mainframe operating system.
- The process for termination of physical access when an individual no longer required access.
- The mass approval and load process for users transitioning to the ERP. (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 & Technology's (Department) controls related to the control objectives stated in the "Description of the IT General Controls and Application Controls for the Department of Innovation & 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 several areas, including modifications to access rights and physical security incident reports. 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.

Exceptions prevented auditors from determining if controls were suitably designed

In addition, during our testing, we noted:
- Change Management Policy & Procedures for ERP did not provide sufficient detail to determine that change requests were properly completed, validated, reviewed, and approved.
- The Department did not maintain documentation of the annual review of security software IDs with powerful privileges.
- The Department did not maintain documentation of the review Incident Reports by the Chief Information Security Officer.
- The Department did not maintain documentation of assessments of newly discovered vulnerabilities.

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 recommend 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 & Technology's (Department) controls related to the control objectives stated in the "Description of the IT General Controls and Application Controls for the Department of Innovation & 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:

Policies and Procedures weaknesses

- Policies and Procedures did not provide guidance related to areas such as prioritization of requests, required approvals, testing and documentation requirements, and requirements for post implementation reviews. In addition, policies and procedures governing logical security did not address the requirements for requesting, obtaining and modifying access rights, periodic review of access rights, and revocation of access rights.

Human Resources weaknesses

- Multiple instances where employees or contractors had not completed security awareness training, cybersecurity training, or the annual acknowledgement of compliance with security policies.

Access provisioning and de-provisioning weaknesses

- Multiple instances where employees or contractors did not have authorization to obtain access rights, request forms were submitted late or not properly approved. In addition, access rights were not always removed timely and separation reports were not always reviewed.

Application Edits weaknesses

- Multiple ERP transaction codes were still active even though they were no longer utilized by the Department, an edit check to prevent duplicate asset tag numbers had not been implemented, and problems with tax tables for other states.

Change Management weaknesses

- Instances where ERP change requests were not properly completed and approved.

Device Configuration weaknesses

- The required security banner warning of prosecution for unauthorized access was not always displayed at initial sign-on. In addition 551 laptops and desktops were not up-to-date with the latest anti-virus product and 3,692 were not up-to-date with the latest anti-virus definitions.

Environmental weaknesses

- A lack of maintenance contracts for generators and an uninterruptable power supply in facilities.

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 11-13 of GAS Report)

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

Department agreed with Service Auditors

Department officials accepted the recommendation.

DEPARTMENT SECRETARY

During Examination Period:
Hardik Bhatt (Designee) (07/01/17 to 09/17/17)
Kirk Lonbom (Acting) (09/18/17 to present)

SERVICE AUDITOR'S OPINION

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

    a. the description does not fairly present the Description of System.

    b. 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.

    c. the controls did not operate effectively to provide reasonable assurance that the control objectives stated in the Description of System were achieved.

This Service Organization Examination was conducted by the Office of the Auditor General's staff.

SIGNED ORIGINAL ON FILE
_____
WILLIAM J. SAMPIAS
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