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

SUMMARY REPORT DIGEST

SUPREME COURT OF ILLINOIS

State Compliance Examination
For the Two Years Ended June 30, 2021

Release Date: July 13, 2022

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

AGING SCHEDULE OF REPEATED FINDINGS

Repeated Since	Category 1	Category 2	Category 3
2019		21-02	

INTRODUCTION

Our compliance examination of the Supreme Court included Appellate Court Districts 1-5 and the Illinois Courts Commission.

SYNOPSIS

- (**21-01**) The Court did not maintain adequate internal controls related to its cybersecurity programs and practices.
- (**21-02**) The Court did not maintain adequate controls over its service providers.

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.

SUPREME COURT OF ILLINOIS
STATE COMPLIANCE EXAMINATION
For the Two Years Ended June 30, 2021

EXPENDITURE STATISTICS	2021	2020	2019
Total Expenditures	**$ 427,378,470**	**$ 409,088,364**	**$ 350,902,660**
OPERATIONS TOTAL	$ 277,474,733	$ 272,836,618	$ 264,771,522
% of Total Expenditures	64.9%	66.7%	75.5%
Personal Services	239,923,720	233,801,996	227,405,324
Other Payroll Costs (FICA, Retirement)	7,445,469	7,234,222	7,046,634
All Other Operating Expenditures	30,105,544	31,800,400	30,319,564
AWARDS AND GRANTS	$ 149,889,145	$ 136,240,008	$ 86,127,861
% of Total Expenditures	35.1%	33.3%	24.5%
REFUNDS	$ 14,592	$ 11,738	$ 3,277
% of Total Expenditures	0.0%	0.0%	0.0%
Total Receipts	$ 1,844,373	$ 1,737,423	$ 1,610,595
Average Number of Employees	**1,562**	**1,550**	**1,552**

AGENCY DIRECTOR
During Examination Period: Marcia M. Meis
Currently: Marcia M. Meis

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

WEAKNESSES IN CYBERSECURITY PROGRAMS AND PRACTICES

The Court did not maintain adequate internal controls related to its cybersecurity programs and practices.

During our examination of the Court's cybersecurity programs and practices, we noted the Court had not:

Policies and procedures lacking

- Established policies and procedures governing the controls related to the onboarding of staff and contractors.
- Ensured all staff and contractors received and acknowledged receipt of the security policies at least annually.

Annual cybersecurity training not provided

- Provided cybersecurity training to staff and contractors upon hiring and annually thereafter.

Court lacked a comprehensive risk assessment

- Developed a project management framework to ensure new applications were adequately developed and implemented in accordance with management's expectations.
- Developed a comprehensive system development methodology.
- Developed a comprehensive cybersecurity plan.
- Developed a risk management methodology, conducted a comprehensive risk assessment, or implemented risk reducing controls.
- Developed a data classification methodology.
- Developed procedures for implementing and monitoring identified vulnerabilities. (Finding 1, pages 10-12)

We recommended the Court:

- Establish policies and procedures governing the controls related to the onboarding of staff and contractors.
- Ensure all staff and contractors receive and acknowledge receipt of the security policies at least annually.
- Provide cybersecurity training to staff and contractors upon hiring and annually thereafter.
- Develop a project management framework to ensure new applications are adequately developed and implemented in accordance with management's expectations.
- Develop a comprehensive system development methodology, including details on the development phases, documentation requirements, user testing requirements and management approvals.
- Develop a comprehensive cybersecurity plan.

- Develop a risk management methodology, conduct a comprehensive risk assessment, and implement risk reducing controls.
- Develop a data classification methodology, including data classifications and details on determining the classifications are adequately secured.
- Develop procedures for implementing and monitoring identified vulnerabilities.

Court partially agreed

Management stated the Court agrees with limited parts of the finding and will continue to follow best practices to enhance its documentation and planning. Management also stated the audit finding as drafted does not acknowledge or reference the Court's many cybersecurity protocols and procedures that are in place.

Court failed to provide documentation to support controls in place

In an accountant's comment, the accountants stated the Court failed to provide documentation to support the controls in place. The lack of documentation hinders our ability to review and assess the Court's cybersecurity program and practices.

INADEQUATE CONTROLS OVER THE REVIEW OF INTERNAL CONTROLS OVER SERVICE PROVIDERS

The Court did not maintain adequate controls over its service providers.

The Court did not provide documentation demonstrating their listing of service providers was complete and accurate. Due to these conditions, we are unable to conclude the Court's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.35).

We performed testing over the one service provider identified by the Court. During our testing we noted for the period of July 1, 2020 through June 30, 2021, the Court had not:

SOC report not obtained and analyzed for Fiscal Year 2021

- Obtained a System and Organization Control (SOC) report.
- Conducted an analysis of the Complementary User Entity Controls (CUECs).
- Obtained and reviewed SOC reports for subservice organizations or performed alternative procedures to determine the impact on its internal control environment. (Finding 2, pages 13-14)

We recommended the Court implement controls to identify and document all service providers utilized. We also recommended the Court obtain SOC reports annually. We further recommend the Court:

- Monitor and document the operation of the CUECs related to the Court's operations.

- Either obtain and review SOC reports for subservice organizations or perform alternative procedures to satisfy itself the existence of the subservice organization would not impact the internal control environment.
- Document its review of the SOC reports and review all significant issues with subservice organizations to ascertain if a corrective action plan exists and when it will be implemented, any impact to the Court, and any compensating controls.

Court disagreed

Court management disagreed with the finding and stated the Court performs System and Organization Control (SOC) reviews for service organizations, which analyzes all service providers contracted by the Court's IT division. Contracts and vendor lists are reviewed to obtain a list of all potential service organizations. An assessment is completed for the service organizations, including an analysis of subservice organizations, to distinguish between service organizations and vendors. SOC reports are then reviewed and analyzed for all service organizations to ensure that controls exist and relate to the services provided.

Court did not provide SOC reports or analysis of SOC reports for Fiscal Year 2021

An accountant's comment stated although the Court reviewed the Fiscal Year 2020 SOC report performed by an independent service auditor, we were not provided the SOC reports or their analysis of the SOC reports for Fiscal Year 2021.

ACCOUNTANT'S OPINION

The accountants conducted a State compliance examination of the Court for the two years ended June 30, 2021, as required by the Illinois State Auditing Act. The accountants stated the Agency complied, in all material respects, with the requirements described in the report.

This State compliance examination was conducted by Adelfia LLC.

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:lkw