STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES

STATE COMPLIANCE EXAMINATION

For the Year Ended June 30, 2022

Performed as Special Assistant Auditors
for the Auditor General, State of Illinois

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
STATE COMPLIANCE EXAMINATION
For the Year Ended June 30, 2022

TABLE OF CONTENTS

State Compliance Examination Report **Page**

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
STATE COMPLIANCE EXAMINATION
For the Year Ended June 30, 2022

AGENCY OFFICIALS

Comptroller	Susana A. Mendoza
Assistant Comptroller - Chicago Office	Cesar Orozco
Assistant Comptroller - Fiscal Policy and Budget	Kevin Schoeben
Assistant Comptroller - Operations and Information Technology	Ellen M. Andres
Chief Internal Auditor	
July 1, 2021 – November 18, 2021	Gary Shadid
November 19, 2021 – January 13, 2022	Vacant
January 14, 2022 – September 16, 2022	Marvin Becker
September 17, 2022 – current	Teri L. Taylor
Chief Legal Counsel	Debjani Desai

AGENCY OFFICES

The Office's primary administrative offices are located at:

Capitol Building
201 State Capitol
Springfield, Illinois 62706-0001

Land of Lincoln Building
325 West Adams Street
Springfield, Illinois 62704-1871

On June 1, 2022, the Office of Comptroller relocated the Chicago Office from Randolph Street to Monroe Street.

James R. Thompson Building
100 West Randolph Street, Suite 15-500
Chicago, Illinois 60601-3252

555 West Monroe Street
Suite 1400S-A
Chicago, Illinois 60661-3713

ILLINOIS OFFICE OF COMPTROLLER

SUSANA A. MENDOZA
COMPTROLLER

MANAGEMENT ASSERTION LETTER

February 24, 2023

Sikich LLP
132 South Water Street, Suite 300
Decatur, IL 62523

Ladies and Gentlemen:

We are responsible for the identification of, and compliance with, all aspects of laws, regulations, contracts, or grant agreements that could have a material effect on the operations of the State of Illinois, Office of Comptroller – Fiscal Officer Responsibilities (Office). We are responsible for and we have established and maintained an effective system of internal controls over compliance requirements. We have performed an evaluation of the Office's compliance with the following specified requirements during the one-year period ended June 30, 2022. Based on this evaluation, we assert that during the year ended June 30, 2022, the Office has materially complied with the specified requirements listed below.

A. The Office has obligated, expended, received, and used public funds of the State in accordance with the purpose for which such funds have been appropriated or otherwise authorized by law.

B. The Office has obligated, expended, received, and used public funds of the State in accordance with any limitations, restrictions, conditions, or mandatory directions imposed by law upon such obligation, expenditure, receipt, or use.

C. The Office has complied, in all material respects, with applicable laws and regulations, including the State uniform accounting system, in its financial and fiscal operations.

D. State revenues and receipts collected by the Office are in accordance with applicable laws and regulations and the accounting and recordkeeping of such revenues and receipts is fair, accurate, and in accordance with law.

555 West Monroe Street, 1400S-A
Chicago, Illinois 60661-3713
(312) 814-2451

201 State Capitol
Springfield, Illinois 62706-0001
(217) 782-6000

325 West Adams Street
Springfield, Illinois 62704-1871
(800) 877-8078

E. Money or negotiable securities or similar assets handled by the Office on behalf of the State or held in trust by the Office have been properly and legally administered, and the accounting and recordkeeping relating thereto is proper, accurate, and in accordance with law.

Yours truly,

State of Illinois Office of Comptroller – Fiscal Officer Responsibilities

SIGNED ORIGINAL ON FILE

Susana Mendoza, Comptroller

SIGNED ORIGINAL ON FILE

Ellen Andres, Assistant Comptroller | Operations and Information Technology

SIGNED ORIGINAL ON FILE

Debjani Desai, Chief Legal Counsel

STATE COMPLIANCE REPORT

SUMMARY

The State compliance testing performed during this examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants; the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States; the Illinois State Auditing Act (Act); and the *Audit Guide.*

ACCOUNTANT'S REPORT

The Independent Accountant's Report on State Compliance and on Internal Control Over Compliance does not contain scope limitations or disclaimers but does contain a modified opinion on compliance and identifies material weaknesses over internal control over compliance.

SUMMARY OF FINDINGS

Number of	Current Report	Prior Report
Findings	6	1
Repeated Findings	1	1
Prior Recommendations Implemented or Not Repeated	0	0

SCHEDULE OF FINDINGS

Item No.	Page	Last/First Reported	Description	Finding Type
			Current Findings	
2022-001	9	2021/2009	Late payment of statutorily mandated transfers	Material Noncompliance
2022-002	12	New	Failure to implement adequate Information Technology controls	Material Weakness and Material Noncompliance
2022-003	15	New	Inadequate controls over remote access	Significant Deficiency and Noncompliance
2022-004	17	New	Inadequate disaster recovery planning	Significant Deficiency and Noncompliance

Item No.	Page	Last/First Reported	Description	Finding Type
			Current Findings	
2022-005	19	New	Weaknesses in cybersecurity programs and practices	Significant Deficiency and Noncompliance
2022-006	21	New	Inadequate controls over service providers	Significant Deficiency and Noncompliance

EXIT CONFERENCE

The Office waived an exit conference in a correspondence from Ms. Teri Taylor, Chief Internal Auditor, on February 8, 2023.

The responses to the recommendations for items 2022-003 through 2022-006 were provided by Ms. Teri Taylor, Chief Internal Auditor, in a correspondence dated February 9, 2023.

The response to the recommendation for item 2022-001 was provided by Ms. Ellen Andres, Assistant Comptroller – Operations and Information Technology, in a correspondence dated December 9, 2022. The response to the recommendation for item 2022-002 was provided by Ms. Ellen Andres, Assistant Comptroller – Operations and Information Technology, in a correspondence dated December 13, 2022.

SIKICH

CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS
Members of American Institute of Certified Public Accountants

132 South Water St., Suite 300
Decatur, IL 62523
217.423.6000

SIKICH.COM

INDEPENDENT ACCOUNTANT'S REPORT ON STATE COMPLIANCE AND ON INTERNAL CONTROL OVER COMPLIANCE

Honorable Frank J. Mautino
Auditor General
State of Illinois

Report on State Compliance

As Special Assistant Auditors for the Auditor General, we have examined compliance by the State of Illinois, Office of Comptroller – Fiscal Officer Responsibilities (Office) with the specified requirements listed below, as more fully described in the *Audit Guide for Financial Audits and Compliance Attestation Engagements of Illinois State Agencies* (*Audit Guide*) as adopted by the Auditor General, during the year ended June 30, 2022. Management of the Office is responsible for compliance with the specified requirements. Our responsibility is to express an opinion on the Office's compliance with the specified requirements based on our examination.

The specified requirements are:

A. The Office has obligated, expended, received, and used public funds of the State in accordance with the purpose for which such funds have been appropriated or otherwise authorized by law.

B. The Office has obligated, expended, received, and used public funds of the State in accordance with any limitations, restrictions, conditions, or mandatory directions imposed by law upon such obligation, expenditures, receipt, or use.

C. The Office has complied, in all material respects, with applicable laws and regulations, including the State uniform accounting system, in its financial and fiscal operations.

D. State revenues and receipts collected by the Office are in accordance with applicable laws and regulations and the accounting and recordkeeping of such revenues and receipts is fair, accurate, and in accordance with law.

E. Money or negotiable securities or similar assets handled by the Office on behalf of the State or held in trust by the Office have been properly and legally administered, and the accounting and recordkeeping relating thereto is proper, accurate, and in accordance with law.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the Illinois State Auditing Act (Act), and the *Audit Guide*. Those standards, the Act, and the *Audit Guide* require that we plan and perform the examination to obtain reasonable assurance about whether the Office complied with the specified requirements in all material respects. An examination involves performing procedures to obtain evidence about whether the Office complied with the specified requirements. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material noncompliance with the specified requirements, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our modified opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination does not provide a legal determination on the Office's compliance with the specified requirements.

Our examination disclosed material noncompliance with the following specified requirements applicable to the Office during the year ended June 30, 2022. As described in the accompanying Schedule of Findings as item 2022-001, the Office had not obligated, expended, received, and used public funds of the State in accordance with any limitations, restrictions, conditions, or mandatory directions imposed by law upon such obligation, expenditure, receipt, or use. Additionally, as described in the accompanying Schedule of Findings as item 2022-002, the Office had not complied, in all material respects, with applicable laws and regulations.

In our opinion, except for the material noncompliance with the specified requirements described in the preceding paragraph, the Office complied with the specified requirements during the year ended June 30, 2022, in all material respects. However, the results of our procedures disclosed instances of noncompliance with the specified requirements, which are required to be reported in accordance with criteria established by the *Audit Guide* and are described in the accompanying Schedule of Findings as items 2022-003 through 2022-006.

The Office's responses to the compliance findings identified in our examination are described in the accompanying Schedule of Findings. The Office's responses were not subjected to the procedures applied in the examination and, accordingly, we express no opinion on the responses.

The purpose of this report is solely to describe the scope of our testing and the results of that testing in accordance with the requirements of the *Audit Guide*. Accordingly, this report is not suitable for any other purpose.

Report on Internal Control Over Compliance

Management of the Office is responsible for establishing and maintaining effective internal control over compliance with the specified requirements (internal control). In planning and performing our examination, we considered the Office's internal control to determine the examination procedures that are appropriate in the circumstances for the purpose of expressing

our opinion on the Office's compliance with the specified requirements and to test and report on the Office's internal control in accordance with the *Audit Guide*, but not for the purpose of expressing an opinion on the effectiveness of the Office's internal control. Accordingly, we do not express an opinion on the effectiveness of the Office's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying Schedule of Findings, we did identify certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, noncompliance with the specified requirements on a timely basis. A material weakness in internal control is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material noncompliance with the specified requirements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying Schedule of Findings as item 2022-002 to be a material weakness.

A significant deficiency in internal control is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying Schedule of Findings as items 2022-003 through 2022-006 to be significant deficiencies.

As required by the *Audit Guide*, immaterial findings excluded from this report have been reported in a separate letter.

The Office's responses to the internal control findings identified in our examination are described in the accompanying Schedule of Findings. The Office's responses were not subjected to the procedures applied in the examination and, accordingly, we express no opinion on the responses.

The purpose of this report is solely to describe the scope of our testing of internal control and the results of that testing based on the requirements of the *Audit Guide*. Accordingly, this report is not suitable for any other purpose.

SIGNED ORIGINAL ON FILE

Decatur, Illinois
February 24, 2023

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
SCHEDULE OF FINDINGS – CURRENT FINDINGS
Year Ended June 30, 2022

2022-001. **FINDING** (Late payment of statutorily mandated transfers)

The Office of Comptroller (Office) did not ensure all statutorily mandated transfers between State funds were made within established timeframes, as required.

The Office had a system in place to identify and record inter-fund transfers it was required to make. During the fiscal year ended June 30, 2022, the Office timely recorded, within the Statewide Accounting Management System (SAMS), the receivables and related payables for transfers of money in the State Treasury to be made between State of Illinois' funds. However, not all transfers were made timely. During fiscal year 2022, we noted 320 transfers between State funds made greater than 30 days after the statutorily mandated transfer date. Transfers made between one and 30 days after the statutorily mandated transfer date were excluded from the information provided in the following table. The following summary concerning late payment of statutorily mandated transfers highlights the delays of making such transfers in fiscal year 2022 compared to fiscal year 2021 and fiscal year 2020:

	Fiscal Year 2022*	**Fiscal Year 2021****	**Fiscal Year 2020****
Number of late transfers	320 transfers (165 from General Revenue Fund (GRF))	346 transfers (185 from GRF)	323 transfers (170 from GRF)
Range of days transfers were late	31 to 365 days	31 to 398 days	31 to 443 days
Total volume of late transfers, in $	$1.25 billion ($332.52 million from GRF)	$1.28 billion ($355 million from GRF)	$1.20 billion ($339 million from GRF)
Late transfers outstanding and paid after June 30	$876.84 million ($49.69 million from GRF)	$1.07 billion ($162 million from GRF)	$999.41 million ($275 million from GRF)

**Analysis prepared as of October 12, 2022, for fiscal years 2022.*
***Denotes information from the prior year finding.*

Also, during fiscal year 2022, we noted 71 late transfers, totaling $156.17 million, between State funds made between one and 30 days after the statutorily mandated transfer date.

Furthermore, the following table contains the number and amount of late transfers still outstanding as of October 12, 2022, relating to fiscal years 2022, 2021 and 2020.

	Fiscal Year 2022	Fiscal Year 2021	Fiscal Year 2020
Number of late transfers outstanding as of 10/12/2022	130	67	4
Amount of late transfers outstanding as of 10/12/2022	$873.82 million	$544.06 million	$51.62 million

The transfers noted above are mandated by various State statutes that contain the required funds, amounts, and timeline. This finding was first reported during the fiscal year 2009 financial audit.

Office management stated, as they did during the prior examinations, due to continued fiscal circumstances outside the control of the Office, the Office must continue to engage in cash management strategies maximizing the use of State funds while also managing resources on-hand to address various pending vouchers causing some transfers to remain in the SAMS queue until the Office is able to process them.

Office management further stated although it has significantly decreased the payment cycle and the number of late payments by managing revenues on-hand, some transfers cannot be made timely since payments for core State programs are prioritized. Office management also stated the Office policy was to prioritize State obligations for payrolls, pension contributions, human and social services programs, education, and debt service rather than to transfer revenues into funds that have no current demand or funding pressures.

Failure to make inter-fund transfers within applicable timeframes represents noncompliance with State law, and untimely transfers of monies may have delayed the receiving fund's use of appropriated funds. (Finding Code No. 2022-001, 2021-001, 2020-001, 2019-001, 2018-001, 2017-001, 2016-001, 2015-001, 2014-001, 2013-001, 12-1, 11-1, 10-1, 09-1)

RECOMMENDATION

We recommend the Office make transfers within timeframes established by applicable statutes. While we realize the lack of available funds in the State Treasury requires prioritization and cash management decisions, we recommend the Office continue in its efforts to make transfers in as timely a manner as possible.

OFFICE RESPONSE

The Office accepts the recommendation and will continue in its effort to make the required transfers timely but given all the competing payments from limited resources in the State Treasury there will always be some that are late. The Office staff continues to collaborate with various State fiscal officers on regular ongoing basis to complete fund transfers that are essential throughout the fiscal year to avoid disruptions in the delivery of State services or programs.

2022-002. **FINDING** **(**Failure to implement adequate Information Technology controls)

The Office of Comptroller (Office) failed to implement adequate general Information Technology (IT) controls related to its environment and applications.

In order to fulfill its mission as the Comptroller of the State of Illinois, the Office maintains an information technology environment to host its applications and data. To ensure the internal controls over the environment and applications were appropriate, we reviewed the Office's following general IT controls: security of the environment, controls over access provisioning and controls over changes. Our testing noted:

Security of the environment
The Office was unable to provide certain requested information covering the audit period concerning the network and related security policies and procedures. In addition, during our review of the documentation that was provided, we noted instances where the network's security settings were not current or configured.

Controls over access provisioning
During our testing of the Office's controls over access provisioning, we noted instances where the Office:

- Had not established policies and procedures documenting requirements for reviewing security logging reports for the network or their various applications.
- Had not established policies and procedures documenting the process for terminating external users' access.
- Did not document its review of mainframe security violation reports.
- Did not document approval for users' access to applications.
- Did not timely terminate separated users' access.
- Did not conduct a periodic review of users' access to the environment and applications.

Controls over changes
Our review of the Office's System Development Methodology, System Request Procedures, and Network Change Authorization Form Procedures noted they were not current and did not reflect the Office's process for change management.

We requested the Office's population of changes to its network environment. However, the Office was unable to provide a complete and accurate population of changes, as the Office did not require all changes to follow the change management process. As a result, we were unable to test changes to the network.

In addition, we tested a sample of application changes, noting instances of:

- Systems requests and data fixes that were missing documentation of all required approvals, and
- Post Implementation Reviews that were not completed.

Further, in order to determine whether the Office maintained proper segregation of duties over network application changes, we requested the population of developers. In response to our request, the Office provided numerous different listings; however, the Office did not provide documentation demonstrating any of the listings were complete and accurate.

Due to these conditions, we were unable to conclude the Office's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AU-C § 500.08).

Even given the population limitations noted above, we tested a sample of application changes to ensure proper segregation of duties. We noted in our testing that developers migrated the change into the production environment, or sufficient documentation was not provided to determine who conducted the migration.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Access Control, Configuration, and the System Development Life Cycle sections, require entities to maintain proper internal controls over the security of the environment, access provisioning and change management.

Also, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

Further, the Office's Security Administration Guide (Guide) requires the users' supervisor to provide approvals for access and also requires separated users' access be terminated on the last date of employment. In addition, the Office is to periodically review users' access.

Office management indicated that missing information causing the auditors to cite security weaknesses was due to insufficient written documentation of current processes and procedures.

Inadequate controls over the Office's environment and applications could lead to unauthorized access, unauthorized changes and security risks to its environment, applications and related data. Also, due to the severity of the weaknesses noted, we were unable to rely upon the general IT control over the environment and applications. (Finding Code No. 2022-002)

RECOMMENDATION

We recommend the Office implement adequate general IT controls related to its environment and applications.

OFFICE RESPONSE

The Office accepts the recommendation. The policies and procedures should be reviewed and updated to ensure they reflect current practices. The Office must be agile in its operations to ensure statutory requirements are met and adapts, as necessary, when conditions change. Although the Office was not always timely in terminating separated users' access from specific applications, all employees leaving employment with the Office are terminated from the network on their last day. This practice can be clarified with a procedure change. The Office will continue to work to timely update procedures and ensure the required supporting documentation is maintained in accordance with the documented procedures in place.

2022-003. **FINDING** (Inadequate controls over remote access)

The Office of Comptroller (Office) did not maintain adequate controls over remote access to its environment, applications and data.

As a result of the COVID-19 pandemic, the Office staff continued to perform work from their home. To enable staff to work from home, the Office allowed staff remote access to its environment, applications and data. Our review of the Office's controls over remote access noted the Office had not:

- Established policies and procedures to control remote access.
- Communicated requirements to users.
- Periodically reviewed users' remote access.
- Maintained documentation demonstrating the information technology equipment utilized contained updated antivirus and the latest security patches.
- Maintained documentation multi-factor authentication was utilized.

In addition, we requested remote access approvals for a sample of 40 users. However, the Office did not provide documentation of the approvals.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Access Control and System and Communication Protection sections, requires entities to implement adequate internal controls over access to its environment, applications and data.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

Office management stated they did not have a formalized process to document security controls over remote access.

Without adequate controls over remote access, unauthorized individuals may have access to the environment, applications and data maintained by the Office, which may also result in malicious activity. (Finding Code No. 2022-003)

RECOMMENDATION

We recommend the Office implement controls to ensure the security over remote access to its environment, applications and data. Specifically, we recommend the Office:

- Establish policies and procedures to control remote access.
- Communicate requirements to users.
- Periodically review users' remote access.

- Maintain documentation demonstrating the information technology equipment utilized contained updated antivirus software and the latest security patches.
- Maintain documentation multi-factor authentication was utilized.

Further, we recommend the Office obtain and maintain approval for all users' remote access.

OFFICE RESPONSE

The Office accepts the recommendation. The Office has updated the remote access user agreements to communicate user responsibilities. The Office will formally document the process currently in place for assignment and approval of remote access and establish a process for periodic access reviews. Documentation of antivirus and security will be maintained.

2022-004. **FINDING** (Inadequate disaster recovery planning)

The Office of Comptroller (Office) did not ensure adequate recovery plans were maintained.

The Office was established to maintain the State's central fiscal accounts, order payments into the treasury and issue warrants against any funds held by the Treasurer. In order to meet its mission, the Office utilizes a myriad of applications.

During our review of the Office's Data Center Contingency Plan (Plan), dated June 21, 2021, we noted the Plan:

- Did not contain or reference detailed recovery scripts for the applications,
- Did not document the recovery time objective, and
- Had not been updated as a result of the annual recovery test.

In addition, we noted:

- The Office had not conducted a business impact analysis,
- The Office's Business Continuity Plan had not been reviewed or updated since October 2019,
- The Office's Network Disaster Recovery Outline was outdated, and
- The Office did not provide to us its Network Disaster Recovery Procedures.

The *Contingency Planning Guide for Information Technology Systems* published by the National Institute of Standards and Technology (NIST) requires entities to have an updated and regularly tested disaster contingency plan to ensure the timely recovery of applications and data. In addition, a business impact analysis is a key step in implementing contingency planning controls and processes.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

The Office's Data Center Disaster Contingency Plan states 'to ensure that the disaster contingency plan can be effective in a disaster situation, the plan must be updated, reviewed and tested on a regular basis.'

Office management stated updates to the Data Center Contingency Plan and Business Continuity Plan were overlooked during the period.

Inadequate recovery plans could result in delayed recovery of the Office's operations and affect the Office's ability to fulfill its mission. (Finding Code No. 2022-004)

RECOMMENDATION

We recommend the Office review and update accordingly its Data Center Contingency Plan and Business Continuity Plan at least annually or after recovery testing. We also recommend the Office update the Data Center Contingency Plan to document, or make reference to:

- Detailed recovery scripts for its applications, and
- Recovery time objectives.

Additionally, we recommend the Office conduct a business impact analysis.

OFFICE RESPONSE

The Office accepts the recommendation. The Office is in the process of updating the Business Continuity Plan and will also be updating the Data Center Contingency Plan. Although not referenced within the Data Center Contingency Plan, the Office's Incident Management Plan includes the recovery time objectives and scripts. Further, the Office successfully completed a recovery test and no updates to the Plan were required. While the Office has not formally completed and documented a Business Impact Analysis, the components of the analysis were considered in developing the Office's Incident Management Plan, Data Center Contingency Plan, and Network Disaster Recovery Outline.

2022-005. **FINDING** (Weaknesses in cybersecurity programs and practices)

The Office of Comptroller (Office) had not implemented adequate internal controls related to cybersecurity programs, practices and control of confidential information.

The Office utilizes various applications which contain a significant amount of critical and confidential data, such as names, addresses, Social Security numbers, banking information, etc.

The Illinois State Auditing Act (30 ILCS 5/3-2.4) requires the Auditor General to review State agencies and their cybersecurity programs and practices. During our examination of the Office's cybersecurity programs, practices and control of confidential information, we noted the Office had not:

- Developed policies and procedures related to:
  - Configuration management,
  - Access control for all environments, and
  - Data loss prevention.
- Established a schedule to review and update security policies and procedures.
- Established a data classification methodology or classified its data most susceptible to attack to ensure adequate protection.
- Developed a risk management methodology and implemented risk reducing internal controls related to the risk identified in the Office's risk assessment.
- Communicated the Office's cybersecurity policies to contractors.

The *Framework for Improving Critical Infrastructure Cybersecurity* and the *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST) requires entities to consider risk management practices, threat environments, legal and regulatory requirements, mission objectives and constraints in order to ensure the security of their applications, data and continued business mission.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

Office management indicated the Written Information Security Plan will develop the framework for cybersecurity policies, however, it was not completed during the examination period.

The lack of an adequate cybersecurity program and adequate cybersecurity practices could result in unidentified risks and vulnerabilities, which could ultimately lead to the Office's confidential and personal information being susceptible to cyberattacks and unauthorized disclosure. (Finding Code No. 2022-005)

RECOMMENDATION

We recommend the Office:

- Develop policies and procedures related to:
  - Configuration management,
  - Access control for all environments, and
  - Data loss prevention.
- Establish a schedule to review and update security policies and procedures.
- Establish a data classification methodology and classify its data most susceptible to attack to ensure adequate protection.
- Develop a risk management methodology and implement risk reducing internal controls.
- Communicate the Office's cybersecurity policies to contractors.

OFFICE RESPONSE

The Office accepts the finding. The Office is in the process of updating and completing the draft sections of the Written Information Security Plan to formalize the policies and procedures noted above. In addition, the Office is finalizing a form to document communication and acceptance of security policies for contractors.

2022-006. **FINDING** (Inadequate controls over service providers)

The Office of Comptroller (Office) had not implemented adequate controls over its service providers.

We requested the Office provide the population of service providers utilized during the examination period to determine if the Office had reviewed the internal controls of its service providers. In response to our request, the Office provided a listing; however, the Office did not provide documentation demonstrating the listing was complete and accurate.

Due to these conditions, we were unable to conclude the Office's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.36).

Even given the population limitations noted above, we performed testing over three of six service providers identified by the Office. The Office utilized service providers for hosting services and software as a service.

Our testing noted the Office had not:

- Obtained System and Organization Control (SOC) reports or conducted independent internal control reviews for the three service providers.
- Conducted an analysis to determine the impact of noted deviations within the SOC report.
- Monitored and documented the operation of the Complementary User Entity Controls (CUECs) related to the Office's operations.
- Obtained and reviewed SOC reports for subservice providers or perform alternative procedures to determine the impact on its internal control environment.
- Developed or implemented procedures for monitoring service providers.

We also noted the service providers' contracts did not contain requirements for independent reviews to be conducted.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Maintenance and System and Service Acquisition sections, requires entities outsourcing their information technology environment or operations to obtain assurance over the entities' internal controls related to the services provided. Such assurance may be obtained via System and Organization Control reports or independent reviews.

Office management indicated the failure to formalize procedures to ensure all service providers were identified, assessed, and monitored was due to oversight.

Without having obtained and reviewed SOC reports or another form of independent internal control review, the Office does not have assurance the service providers' internal controls are adequate and operating effectively. (Finding Code No. 2022-006)

RECOMMENDATION

We recommend the Office strengthen its controls in identifying and documenting all service providers utilized. Further, we recommend the Office:

- Obtain SOC reports or conduct independent internal control reviews.
- Conduct an analysis to determine the impact of noted deviations within the SOC report.
- Monitor and document the operation of the CUECs related to the Office's operations.
- Obtain and review SOC reports for subservice providers or perform alternative procedures to determine the impact on its internal control environment.
- Develop and implement procedures for monitoring service providers.
- Ensure the service providers' contract contain requirements for independent reviews to be conducted.

OFFICE RESPONSE

The Office accepts the recommendation. The Office is developing a process and formalizing procedures to identify, obtain, and document review of service organizations.