SIKICH®

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES

STATE COMPLIANCE EXAMINATION

For the Year Ended June 30, 2024

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, 2024

TABLE OF CONTENTS

State Compliance Examination Report **Page**

Agency Officials 1

Management Assertion Letter 2

State Compliance Report
- Summary 4
- Independent Accountant's Report on State Compliance and on Internal Control Over Compliance 6

Schedule of Findings
- Current Findings 9

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
COMPLIANCE EXAMINATION
For the Year Ended June 30, 2024

AGENCY OFFICIALS

Comptroller	Susana A. Mendoza
Assistant Comptroller – Fiscal Policy and Budget	Kevin Schoeben
Assistant Comptroller – Operations Division	
July 1, 2023 – September 14, 2023	Vacant
September 15, 2023 – May 31, 2024	Kathleen Killion
June 1, 2024 – June 30, 2024	Vacant
July 1, 2024 – current	Melissa Saettler
Assistant Comptroller – Chicago Office	Cesar Orozco
General Counsel/Chief Legal Counsel	
July 1, 2023 – July 13, 2023 (Chief Legal Counsel)	Debjani Desai
July 14, 2023 – current (General Counsel)	Adam Alstott
Chief Internal Auditor	Teri L. Taylor

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

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

ILLINOIS OFFICE OF COMPTROLLER

SUSANA A. MENDOZA
COMPTROLLER

MANAGEMENT ASSERTION LETTER – STATE COMPLIANCE EXAMINATION

February 18, 2025

Sikich CPA LLC
132 South Water Street, Suite 300
Decatur, IL 62523

Dear Sikich:

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, 2024. Based on this evaluation, we assert that during the year ended June 30, 2024, 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. Other than what has been previously disclosed and reported in the Schedule of Findings, 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. Other than what has been previously disclosed and reported in the Schedule of Findings, 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

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 A. Mendoza, Comptroller

SIGNED ORIGINAL ON FILE

Melissa Saettler, Assistant Comptroller, Operations Division

SIGNED ORIGINAL ON FILE

Kevin Schoeben, Assistant Comptroller, Fiscal Policy and Budget

SIGNED ORIGINAL ON FILE

Adam Alstott, General Counsel

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
STATE COMPLIANCE EXAMINATION
For the Year Ended June 30, 2024

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	6
Repeated Findings	6	6
Prior Recommendations Implemented or Not Repeated	0	0

SCHEDULE OF FINDINGS

Item No.	Page	Last/First Reported	Description	Finding Type
			Current Findings	
2024-001	9	2023/2022	Failure to implement adequate Information Technology controls	Material Weakness and Material Noncompliance
2024-002	12	2023/2009	Late payment of statutorily mandated transfers	Material Noncompliance
2024-003	15	2023/2022	Inadequate controls over service providers	Material Weakness and Material Noncompliance

Item No.	Page	Last/First Reported	Description	Finding Type
			Current Findings	
2024-004	17	2023/2022	Inadequate controls over remote access	Significant Deficiency and Noncompliance
2024-005	19	2023/2022	Inadequate disaster recovery planning	Significant Deficiency and Noncompliance
2024-006	21	2023/2022	Weaknesses in cybersecurity programs and practices	Significant Deficiency and Noncompliance

EXIT CONFERENCE

The Office waived an exit conference in a correspondence from Ms. Teri Taylor, Chief Internal Auditor, on February 5, 2025.

The response to the recommendation for item 2024-001 was provided by Ms. Teri Taylor, Chief Internal Auditor, in a correspondence dated December 5, 2024.

The responses to the recommendations for items 2024-002 through 2024-006 were provided by Ms. Melissa Saettler, Assistant Comptroller, Operations Division, in a correspondence dated February 18, 2025.

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, 2024. 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, 2024. As described in the accompanying Schedule of Findings as item 2024-002, 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 items 2024-001 and 2024-003, 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, 2024, 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 2024-004 through 2024-006.

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 items 2024-001 and 2024-003 to be material weaknesses.

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 2024-004 through 2024-006 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 18, 2025

2024-001. **FINDING** (Failure to implement adequate Information Technology controls)

The Office of Comptroller (Office) did not 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 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, the Office was unable to provide a complete and accurate population of network devices for detailed testing. 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).

Despite this limitation, we performed testing on a sample of network devices and noted instances where the network security settings were not current or properly configured.

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

- Three of nine (33%) users had access to critical applications when their job descriptions did not require such access.
- The Office had not established a formal process to periodically review users' access to the applications.
- The Office had not conducted periodic reviews of users' permissions to the Active Directory system.

Controls over changes
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. 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).

Despite this limitation, we performed testing on a sample of network changes and noted documentation of change approvals were not maintained for 18 of 18 (100%) network changes.

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

- Change requests did not have documentation of required approvals for 2 of 17 (12%) changes, and
- Documentation of work-hours was not maintained for 17 of 24 (71%) changes.

This finding was first reported in fiscal year 2022. In subsequent years, the Office has been unsuccessful in implementing procedures to fully remediate the issues identified.

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, System Development Life Cycle, and System and Services Acquisition sections, require entities to maintain proper internal controls over the security of the environments, 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 requires the Office to periodically review users' access. Finally, the Office's System Request Procedures require appropriate approvals and work-hours documentation for system change requests.

Office management stated the items causing auditors to cite concerns were due to incomplete written documentation although technical controls remain in place. Further, Office management stated staffing shortages limited the Office's ability to implement adequate general IT controls.

Inadequate controls over the Office's environment and applications could lead to unauthorized access, unauthorized changes, and security risks to its environments, applications, and related data. (Finding Code No. 2024-001, 2023-002, 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 Office must be agile in its operations to ensure statutory requirements are met and adapt when conditions change. Over the past year the Office has worked to address the items identified by the auditors and will continue to enhance critical event avoidance controls.

2024-002. **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, 2024, 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 timely made. During fiscal year 2024, we noted 163 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 2024 compared to fiscal year 2023:

	Fiscal Year 2024*	**Fiscal Year 2023****
Number of late transfers	163 transfers (32 from General Revenue Fund (GRF))	264 transfers (127 from GRF)
Range of days transfers were late	34 to 365 days	31 to 299 days
Total volume of late transfers, in $	$1.04 billion ($182.69 million from GRF)	$1.23 billion ($327.98 million from GRF)
Late transfers outstanding and paid after June 30	$448.13 million ($0 from GRF)	$954.86 million ($0 from GRF)

**Analysis prepared as of October 18, 2024, for fiscal year 2024.*

***Denotes information from the prior year finding.*

Also, during fiscal year 2024, we noted 207 late transfers, totaling $539.46 million, between State funds made between one and 30 days after the statutorily mandated transfer date.

Furthermore, the following table contains the number of late transfers still outstanding as of October 18, 2024, relating to fiscal years 2024 and 2023. No outstanding transfers were noted prior to fiscal year 2023.

	Fiscal Year 2024	Fiscal Year 2023
Number of late transfers outstanding as of 10/18/2024	62	6
Amount of late transfers outstanding as of 10/18/2024	$335.60 million	$47.35 million

The transfers noted above are mandated by various State statutes containing the required funds, amounts, and timeline.

This finding was first reported during the fiscal year 2009 compliance examination. While making improvements in subsequent years, the Office has been unsuccessful in implementing procedures to remediate the issues identified.

Office management stated, as they did during 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. 2024-002, 2023-001, 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 transfers pending until funds are available, or when needed. It should be noted that most GRF transfers were made by the end of June 30, 2024 and the few pending GRF transfers were not delayed. Pending non-GRF transfers, especially those for capital obligations, will be processed upon collaboration with the respective State agencies. The Office staff continues to work together with various State fiscal officers on a regular ongoing basis to manage the processing of such transfers throughout the fiscal year to avoid disruptions in the delivery of State services or programs.

2024-003. **FINDING** (Inadequate controls over service providers)

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

We requested the Office's 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 population; however, the population contained an inaccuracy. Due to this condition, 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). Despite the limitation noted above, we selected a sample of service providers for our detailed testing and noted the Office:

- Did not review the System and Organization Controls (SOC) reports for three of three (100%) service providers.
- Did not have a system in place to monitor performance measures or compliance with the contract requirements at the service providers.

This finding was first reported in fiscal year 2022. In subsequent years, the Office has been unsuccessful in implementing procedures to remediate the issues identified.

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 Services 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 Controls reports or independent reviews.

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.

Office management stated staffing shortages resulted in the above conditions identified.

Without maintaining an accurate list of service providers and reviewing 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. In addition, failure to monitor compliance with contract requirements may lead to inadequate services provided by the service providers. (Finding Code No. 2024-003, 2023-006, 2022-006)

RECOMMENDATION

We recommend the Office maintain an accurate list of service providers and review SOC reports covering the examination period. Additionally, we recommend the Office monitor the contracted controls at its service providers to ensure compliance with the contract requirements.

OFFICE RESPONSE

The Office accepts the recommendation. The Office has implemented a process to maintain an authoritative list of service providers and ensure complete review of SOC2 reports or industry standard alternatives. The Office is in the process of finalizing a document to include in future contracts ensuring providers meet security control requirements.

2024-004. **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.

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 comprehensive policies and procedures to adequately address controls over remote access, including user responsibilities and applicable data laws.
- Communicated remote access requirements to users.
- Ensured users completed required remote access acknowledgments.
- Periodically reviewed users' remote access.
- Maintained sufficient documentation demonstrating the security controls over remote access were adequate regarding multi-factor authentication.

This finding was first reported in fiscal year 2022. In subsequent years, the Office has been unsuccessful in implementing procedures to remediate the issues identified.

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 Identification and Authentication 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 the Office has experienced staffing shortages that have led to the conditions found above.

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. 2024-004, 2023-003, 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 comprehensive policies and procedures to address controls over remote access.
- Communicate remote access requirements to users.
- Ensure users complete required remote access acknowledgments.
- Periodically review users' remote access.
- Maintain sufficient documentation demonstrating the security controls over remote access are adequate for multi-factor authentication.

OFFICE RESPONSE

The Office accepts the recommendation and will continue to improve the policies and procedures to control remote access. The Office:

- communicates remote access requirements to users when providing the remote access acknowledgment agreement that is required for every Office employee.
- will review agreements with contractual employees and third-party vendors to ensure the contract language requires individuals to follow all Office policies, including remote access policies.
- has established a schedule to review users' remote access rights.
- is in the process of documenting security controls over remote access and multi-factor authentication.

2024-005. **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, we noted the Office conducted a disaster recovery test in May 2024. However, the documentation of testing and test results had not been finalized during fiscal year 2024.

Additionally, during our review of the Office's business impact analysis, we noted the Office did not document MTD (Maximum Tolerable Downtime), RPO (Recovery Point Objective), and RTO (Recovery Time Objective) for all of its critical business processes, systems and applications.

This finding was first reported in fiscal year 2022. In subsequent years, the Office has been partially successful in implementing procedures to remediate the issues identified.

The *Contingency Planning Guide for Federal Information Systems* published by the National Institute of Standards and Technology (NIST) requires entities to have an updated and regularly (at least annually) tested disaster contingency plan to ensure the timely recovery of applications and data. In addition, a detailed 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.

Office management stated required documentation was not timely completed due to timing constraints of staff.

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. 2024-005, 2023-004, 2022-004)

RECOMMENDATION

We recommend the Office timely finalize their disaster recovery testing documentation. Additionally, we recommend the Office update the business impact analysis to identify RPO, RTO, and MTD for all of its critical business processes, systems and applications.

OFFICE RESPONSE

The Office accepts the recommendation. The Office annually reviews and updates the business impact analysis as appropriate. Before FY25, the recovery point objectives (RPO), recovery time objectives (RTO), and maximum tolerable downtime (MTD) were documented in the other disaster recovery documentation provided annually to auditors. Going forward, these metrics will be added to the business impact analysis for the convenience of reviews and audits. The Office will continue to improve exercises with individual application teams to collect recovery point objectives (RPO), recovery time objectives (RTO), maximum tolerable downtime (MTD), and other metrics to inform and update the business continuity and disaster recovery plans.

2024-006. **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,
  - data loss prevention,
  - firewall and network device controls, and
  - virus detection.
- 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.
- Established a project management framework.

Further, the Office was unable to maintain a complete and accurate population of system users for one of their critical applications.

This finding was first reported in fiscal year 2022. In subsequent years, the Office has been unsuccessful in implementing procedures to remediate the issues identified.

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 stated the staffing shortages and competing priorities resulted in the conditions noted above.

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. 2024-006, 2023-005, 2022-005)

RECOMMENDATION

We recommend the Office:

- Develop policies and procedures related to:
  - configuration management,
  - access control for all environments,
  - data loss prevention,
  - firewall and network device controls, and
  - virus detection.
- 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.
- Establish a project management framework.
- Maintain a complete and accurate population of system users for critical applications.

OFFICE RESPONSE

The Office accepts the recommendation. The Office has hired a Chief Information Security Officer and staffed a new cybersecurity unit within its IT division.

This unit is implementing a risk management framework informed by the NIST Cybersecurity Framework 2.0. This effort will address introducing new policies, establishing an effective policy review/update schedule, introducing a data classification strategy, and be working toward unifying identity and access management for critical applications.

The Office is finalizing a project management framework to define system changes and implementations that exceed routine updates or enhancements.