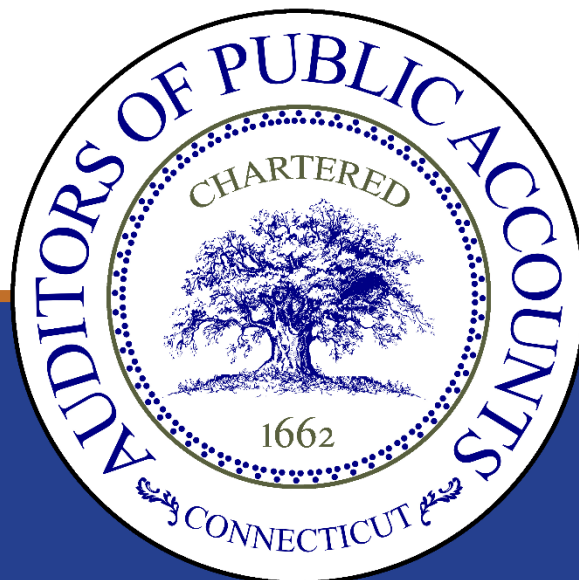


AUDITORS' REPORT

STATE DATA CENTER GENERAL CONTROLS

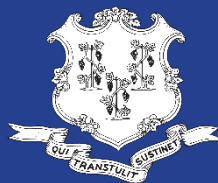
Office of the Treasurer

AS OF MAY 2022



STATE OF CONNECTICUT
Auditors of Public Accounts

JOHN C. GERAGOSIAN
State Auditor



CLARK J. CHAPIN
State Auditor

CONTENTS

INTRODUCTION..... 3

AUDIT-AT-A-GLANCE 4

STATE AUDITORS’ FINDINGS AND RECOMMENDATIONS..... 5

 Unlocked Server Cabinets (Security) 5

 Treasurer IT Staffing Levels (Personnel) 6

 Lack of Data Classification Assessment (Planning) 7

 Lack of Formal IT Documentation (Planning)..... 8

OBJECTIVES, SCOPE, AND METHODOLOGY 10

ABOUT THE AUDIT 12

STATE OF CONNECTICUT



AUDITORS OF PUBLIC ACCOUNTS

JOHN C. GERAGOSIAN

STATE CAPITOL
210 CAPITOL AVENUE
HARTFORD, CONNECTICUT 06106-1559

CLARK J. CHAPIN

July 20, 2023

INTRODUCTION

We are pleased to submit this audit of the Office of the Treasurer as of May 2022 in accordance with the provisions of Section 2-90 of the Connecticut General Statutes. Our audit identified internal control deficiencies; apparent non-compliance with policies and procedures; and a need for improvement in management practices and procedures that we deemed to be reportable.

The Auditors of Public Accounts wish to express our appreciation for the courtesies and cooperation extended to our representatives by the personnel of the Office of the Treasurer during the course of our examination.

The Auditors of Public Accounts also would like to acknowledge the auditors who contributed to this report:

Jared Kolomyjec
Joan Main

A handwritten signature in black ink, appearing to read "C. D'Amico".

Christopher D'Amico
Principal Auditor

Approved:


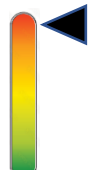
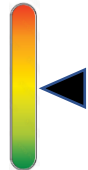
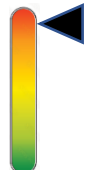
A handwritten signature in black ink, appearing to read "John C. Geragosian".

John C. Geragosian
State Auditor

A handwritten signature in black ink, appearing to read "Clark J. Chapin".

Clark J. Chapin
State Auditor

AUDIT-AT-A-GLANCE

Category	Audit Risk	Description
Maintenance	 Low	Maintenance controls concern how well agencies keep their information technology (IT) systems up to date, patched, and operational. Our review noted that the Office of the Treasurer consistently monitors its servers, keeps them up to date, and appropriately patches them. This engagement did not note any related findings or recommendations.
Personnel	 High	Personnel controls identify how well the IT group is staffed, aware of its responsibilities, and able to perform its duties. Current staff, which includes several retirement-eligible individuals, will be unable to provide continuous and reliable support to the Office of the Treasurer in the future. The Office of the Treasurer should maintain adequate information technology staffing levels to ensure continued and stable operations and provide for knowledge retention and succession planning.
Planning	 Moderate	<p>Planning controls indicate how well IT systems are insulated from disruption, unauthorized access, and similar events that might detrimentally impact operations. The Office of the Treasurer did not classify its information systems and data. The office should conduct a comprehensive data classification assessment in accordance with Office of Policy and Management policy.</p> <p>The Office of the Treasurer maintains formal, written descriptions and guides of its major systems. However, the office is missing some or all documentation for its other systems and functions, including its older and internally developed applications. The Office of the Treasurer should finish codifying and documenting its information technology procedures and systems to minimize the risk of knowledge loss and improve training outcomes.</p>
Security	 High	Security controls identify how well IT systems are protected (physically and logically) and ensure an agency's data are backed up and accessible. Our walkthrough and inspection of server storage space disclosed several unlocked server racks. We also found that the office's compensating controls did not appear to otherwise reduce this risk. The Office of the Treasurer should strengthen internal controls to ensure that it locks computer server racks at all times to protect hardware from unauthorized access or modification.

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our examination of the information technology general controls of the Office of the Treasurer disclosed the following four recommendations.

Finding 1 **Unlocked Server Cabinets (Security)**

Criteria	Although computer servers restrict access to digital systems and resources to authorized users, sufficient physical controls over devices are also necessary to ensure a reliable and stable environment for those operations, especially in computer rooms with shared space.
Condition	Our walkthrough and inspection of server storage space disclosed several unlocked server racks. We also found that the office's compensating controls did not appear to otherwise reduce this risk.
Context	Server racks enable efficient storage in data centers, allowing for adequate airflow, power, and network cabling to devices while providing a stable and reasonably secure platform in which those devices are housed.
Effect	Direct physical access to servers could compromise the integrity, availability, and confidentiality of their stored data. Furthermore, it would be difficult to detect and trace such physical tampering of servers and devices.
Cause	During the move to the current data center location, building management recommended against physical keys to lock each server rack in favor of identification swipe cards for the data center.
Prior Audit Finding	This finding has not been previously reported.
Recommendation	The Office of the Treasurer should strengthen internal controls to ensure that it locks computer server racks at all times to protect hardware from unauthorized access or modification.

Agency Response

"The Office of the Treasurer (OTT) concurs with this finding and will strengthen controls to ensure that computer server racks are locked at all times to protect hardware from unauthorized access or modification.

It should also be noted that changes are being considered regarding future management of the OTT servers that will enhance security. These include moving servers to the cloud or to the Department of Administrative Services/Bureau of Information Technology Solutions (DAS/BITS) data center.

The OTT is currently actively recruiting a new Manager of Information Technology to advise the OTT on these decisions regarding management of servers. Interviews of candidates are currently underway."

Finding 2

Treasurer IT Staffing Levels (Personnel)

Criteria

Maintaining good internal controls over information technology depends upon a knowledgeable and sufficient staff to ensure that its computer operations remain reliable and available to all Office of the Treasurer employees.

Condition

The present composition of the Office of the Treasurer's IT personnel has reached a critical level. Current staff, which includes several retirement-eligible individuals, will be unable to provide continuous and reliable support to other Office of the Treasurer staff in the future.

Context

The Office of the Treasurer has 121 employees, only four of whom serve in an IT capacity. To accomplish its mission, the office must access bank, financial institution, and internal systems. The loss of IT personnel could cause significant operating issues for the Treasurer.

Effect

Without sufficient IT personnel, it would be increasingly difficult to maintain stable IT operations. Insufficient staffing could result in the inability to maintain a stable and secure operating environment, respond to changes in technology, and recover from unforeseen events.

Cause

Unfilled positions and years of shifting priorities away from IT contributed to this condition.

Prior Audit Finding

This finding has not been previously reported.

Recommendation

The Office of the Treasurer should maintain adequate information technology staffing levels to ensure continued and stable operations and provide knowledge retention and succession planning.

Agency Response

"The OTT concurs with this recommendation. Current IT staffing levels are low but the OTT is actively recruiting a new Manager of Information Technology to advise on IT systems and staffing for the OTT. Interviews of candidates are currently underway. In addition, a posting for an Analyst II position will be going out shortly. The OTT plans to fill the Manager of IT position before filling any other open IT position or requesting additional staffing that may be needed.

One option that may be considered is to rely more heavily on BITS to assist with IT requirements of OTT. The head of BITS, Mark Raymond, visited with senior Treasury management and OTT IT staff earlier this year to discuss this option."

Finding 3

Lack of Data Classification Assessment (Planning)

Criteria

The Office of Policy and Management (OPM) requires each executive branch agency to assign a classification to all data over which that agency has custodial responsibility. Regular data classification assessments ensure that statewide information technology resources are appropriately allocated for planning, system design and development, and necessary recovery operations. This affords state agencies a mechanism to better utilize resources and triage systems and data, thereby ensuring continued focus on assets from most to least critical.

Condition

The Office of the Treasurer did not classify its information systems and data.

Context

Each executive agency assigns a category and impact level to each data set in its custody, based on a federal data security matrix. The three federal security objectives (confidentiality, integrity, and accessibility) identify the parameters of information system reliability, and are matched with low, moderate, and high levels of risk for each objective. Completion of this exercise for each data set at an agency ultimately establishes an overall criticality assessment, based on the most critical information system. The Office of the Treasurer maintains or coordinates access to approximately forty internal and external information systems.

Effect

Lack of data classification could result in inefficiencies in assigning operational resources.

Cause	Noncompliance with this policy appears to be a lack of oversight by management.
Prior Audit Finding	This finding has not been previously reported.
Recommendation	The Office of the Treasurer should conduct a comprehensive data classification assessment in accordance with Office of Policy and Management policy.
Agency Response	"The OTT concurs with this finding. The new OTT IT Manager will be tasked with revisiting this matter and engaging with OPM to determine what templates to use based on the attributes of a given data source."

Finding 4

Lack of Formal IT Documentation (Planning)

Criteria	The National Institute of Standards and Technology (NIST) Special Publication 800-53 recommends the need for current and robust procedural and policy documentation as a primary control in each control family.
Condition	The Office of the Treasurer maintains formal, written descriptions and guides of its major information systems. However, the office is missing some or all documentation for its other systems and functions, including its older and internally developed applications.
Context	The Office of the Treasurer currently maintains an IT staff with a strong working knowledge of its operating environment. While the potential impact of lacking such documentation might otherwise be minimized in this circumstance, reliability on this as a compensating control is reduced as staffing levels decrease.
Effect	Potential losses of IT personnel are more likely to create significant downtime and increase the lead time for training new staff, potentially impacting agency operations.
Cause	The Office of the Treasurer has not prioritized documenting policies due to the continuous demand to ensure ongoing stable operations.
Prior Audit Finding	This finding has not been previously reported.

Recommendation

The Office of the Treasurer should finish codifying and documenting its information technology procedures and systems to minimize the risk of knowledge loss and to improve training outcomes.

Agency Response

"OTT disagrees to some extent with this assessment. Most of the OTT major systems are provided by outside vendors who offer the same services to other states and have robust documentation and more leading-edge production deployments and systems that are fully documented. Since this audit was completed, this trend has continued with less and less OTT reliance on internally developed stand-alone systems. Nonetheless, OTT will continue to document systems that still require documentation."

Auditors' Concluding Comments

The Office of the Treasurer has focused its efforts on more critical and widely used systems. Documentation should still be maintained for all systems, especially those whose details may be otherwise lost due to personnel reductions.

OBJECTIVES, SCOPE, AND METHODOLOGY

We have audited certain operations of the Office of the Treasurer in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. The scope of our audit included, but was not necessarily limited to internal controls as of May 2022. The objectives of our audit were to evaluate the:

1. Office's internal controls over significant information technology functions;
2. Office's compliance with policies and procedures internal to the department or promulgated by other state agencies; and
3. Effectiveness, economy, and efficiency of certain management practices and operations.

Our methodology included reviewing written policies and procedures and other pertinent documents; interviewing various personnel of the office; and testing selected transactions. Our testing was not designed to project to a population unless specifically stated. We obtained an understanding of internal controls that we deemed significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We tested internal controls using the National Institute of Standards and Technology's (NIST) Special Publication 800-53 - "Security and Privacy Controls for Information Systems and Organizations" as a guide. This publication includes internal controls that provide a comprehensive foundation for an organization's information security. We used this publication to plan the audit testing performed for this engagement.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The accompanying agency overview is presented for informational purposes. This information was obtained from various available sources including, but not limited to, the office's management and the state's information systems, and was not subjected to the procedures applied in our audit of the office. For the areas audited, we identified:

1. Deficiencies in internal controls;
2. Apparent non-compliance with policies, and procedures; and
3. A need for improvement in management practices and procedures that we deemed to be reportable.

The State Auditors' Findings and Recommendations section of this report presents findings arising from our audit of the Office of the Treasurer. Due to the sensitive nature of the information technology (IT) environment, certain confidential portions of this report and its findings have been omitted to prevent unintentional disclosure of sensitive information. Details of our findings have been provided to agency management for corrective action in a separate communication, which along with its supporting workpapers, are not subject to public disclosure in accordance with Sections 1-210(b)(20) and 2-90(h) of the General Statutes.

ABOUT THE AUDIT

Audit Purpose

We conducted this audit to obtain an understanding of the Office of the Treasurer's data center and its information systems and data. Our review was intended to: (1) identify the design and implementation of the Office of the Treasurer's IT general controls, (2) assess and evaluate those controls and practices against industry standards and state policies and procedures, and (3) identify and communicate opportunities for improvement in the Office of the Treasurer's IT control environment.

Agency Overview

The State Treasurer is one of six state constitutional officers and is responsible for all state financial resources, including monetary receipts, disbursements, investment holdings, and bonding. The Treasurer is also the custodian of the state's pension obligations, debt service, second injury fund, and escheated unclaimed property.

The Office of the Treasurer's IT group oversees all aspects of the agency's computer operations, including desktop support, networking and connectivity, systems access, and coordinating and maintaining servers and information systems thereon. While some such systems are owned and operated by vendors and third parties (e.g., online bank account access), this group supports many in-house platforms. Overall, the IT group administers a critical function for the agency, facilitating much, if not all, of its operations.