STATE OF CONNECTICUT

AUDITORS' REPORT
CORE-CT SYSTEM
INFORMATION TECHNOLOGY GENERAL CONTROLS
AS OF MARCH 2021

AUDITORS OF PUBLIC ACCOUNTS
JOHN C. GERAGOSIAN ❖ CLARK J. CHAPIN

Table of Contents

May 25, 2021

EXECUTIVE SUMMARY

In accordance with the provisions of Section 2-90 of the Connecticut General Statutes, we have audited certain operations of the Core-CT System. Our audit identified internal control deficiencies and the need for changes in management practices that warrant the attention of management. The significant findings and recommendations are presented below:

Page 5	Core-CT staffing levels declined in recent years due to resignations and retirements, and significant positions remain vacant. In addition, Core-CT increased its reliance on third-party consultants and vendors, who often perform tasks that would be performed by agency employees. Core-CT management should maintain sufficient staffing levels to cover current operational needs, reduce reliance on consultants or vendors, and prevent further loss of institutional knowledge through personnel reductions and impending retirements. (Recommendation 1.)
Page 6	Core-CT management has not completed and documented a formal risk assessment for the Core-CT System. Core-CT management should conduct a full fail-over and fail-back test cycle to help ensure preparation for a disaster or other significant detrimental event. (Recommendation 2.)
Page 7	Core-CT has not tested its disaster recovery plan using the full processing demand of all system components. Core-CT management should conduct a test under full production capacity to ensure preparation for a disaster or other significant detrimental event. (Recommendation 3.)
Page 8	There is no agreement between the Office of the State Comptroller and the current provider of the Core-CT disaster recovery hot site location. Core-CT management should enter into a formal agreement for use of the facilities housing the Core-CT disaster recovery hot site. (Recommendation 4.)
Page 8	We interviewed the Office of the State Comptroller personnel responsible for Core-CT staffing and determined that OSC does not perform background checks on newly hired employees who have access to sensitive and classified data. Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT System. (Recommendation 5.)

STATE OF CONNECTICUT

AUDITORS OF PUBLIC ACCOUNTS

State Capitol
210 Capitol Avenue
Hartford, Connecticut 06106-1559

JOHN C. GERAGOSIAN

CLARK J. CHAPIN

May 25, 2021

AUDITORS' REPORT
CORE-CT SYSTEM
INFORMATION TECHNOLOGY GENERAL CONTROLS AUDIT
AS OF MARCH 2021

We have audited certain operations of the Core-CT System, overseen by the Office of the State Comptroller and the Department of Administrative Services, 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, the period ending March 2021. The objectives of our audit were to:

1. Evaluate the system's internal controls over significant management and financial functions;

2. Evaluate the system's compliance with policies and procedures internal to the departments or promulgated by other state agencies, as well as certain legal provisions; and

3. Evaluate the effectiveness, economy, and efficiency of certain management practices and operations, including certain financial transactions.

Our methodology included reviewing written policies and procedures, financial records, minutes of meetings, and other pertinent documents; interviewing various personnel of the department; and testing selected transactions. Our testing is 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. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violations of contracts, grant agreements, or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform our 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 information presented in the Foreword below is for informational purposes. This information was obtained from various available sources including, but not limited to, the departments' management and the state's information systems, and was not subjected to the procedures applied in our audit of the system. For the areas audited, we:

1. Identified deficiencies in internal controls;

2. Did not identify apparent noncompliance with laws, regulations, contracts and grant agreements, policies, and procedures; and

3. Identified need for improvements in management practices and procedures that we deemed to be reportable.

The State Auditors' Findings and Recommendations in the accompanying report presents any findings arising from our audit of the Core-CT System.

COMMENTS

FOREWORD

Organizational Structure

Core-CT is Connecticut's integrated online Human Resources Management System (HRMS) and Financials system. Core-CT was implemented in 2003 to replace numerous older legacy systems to provide standardization, increase ad hoc reporting capabilities, simplify reconciliation, and establish an interactive user environment. Core-CT is comprehensive and includes the state's accounting, purchasing, accounts payable, accounts receivable, project costing, inventory and asset management systems, payroll, benefits, human resources, state and municipal retiree pension tracking, and time and labor functions.

The Office of the State Comptroller (OSC) and the Department of Administrative Services (DAS) jointly administer and maintain the Core-CT System. The system uses enterprise resource planning (ERP) software to incorporate all business functions, using an integrated suite of software applications, common databases, and a unified technical architecture. In addition to standardized reports, the Core-CT System utilizes an Enterprise Performance Management (EPM) ad-hoc reporting function, which allows users to query the data warehouse and produce custom reports.

The Core-CT staff is divided into seven functional teams: Human Resources Management System, Financials, EPM-Ad-Hoc Reporting, Technical, Security, Level 1 Help Desk, and Organizational Readiness. Descriptions of these teams are presented below:

HRMS Team

The HRMS team ensures that the HR modules (i.e., Human Resources, Payroll, Benefits, Pension, and Time and Labor) are configured to meet the state's business process needs. The HRMS team is also responsible for designing, developing, testing, and delivering HR and payroll processing system modifications.

Financials Team

The Financials team ensures that the financials processes modules (i.e., Chart of Accounts, Budgeting, General Ledger, Accounts Payable, Purchasing, Asset Management, Inventory, Accounts Receivable/Billing, Project Costing, and Customer Contracts) meet the state's business process needs. The Financials team is also responsible for designing, developing, testing, and delivering financials system modifications.

EPM-Ad-Hoc Reporting Team

The EPM team is responsible for designing, developing, and delivering an intuitive ad-hoc reporting system for Core-CT. The team administers the statewide data warehouse/information repository that is the technical backbone of the system's advanced enterprise-wide reporting capabilities.

Technical Team

The Technical team is responsible for Core-CT's technology infrastructure. The team manages the selection, configuration, as well as the maintenance of the servers, software, and communication network that form the backbone of Core-CT. The Technical team ensures that the various technical components of Core-CT (i.e., interfaces, security, batch processing, and reporting) are functioning properly, interfacing correctly per system specifications and business needs, and performing at optimal levels.

Core-CT is a collaboration between the Office of the State Comptroller and the Department of Administrative Services. In addition to allocating personnel and infrastructure resources, these agencies share broad authority covering many areas unrelated to the Core-CT System. We focused the agency descriptions to the Core-CT related areas.

Core-CT Project Management Team:

- Martha Carlson, OSC – Deputy State Comptroller
- Mark Raymond, DAS – Chief Information Officer
- Angelo Romano, OSC – Core-CT Director
- Donalynn Black, OSC – Operations & Service Manager
- Glenn Churchill, OSC – Technical Team Manager

Office of the State Comptroller

The Office of the State Comptroller operates primarily under the provisions of Article Fourth, Section 24, of the State Constitution and Title 3, and Chapter 34 of the General Statutes. Under the provisions of Section 3-115a of the General Statutes, the Comptroller provides for the budgetary and financial reporting needs of the executive branch as may be necessary through the Core-CT System.

In addition to the Core-CT organizational reporting structure, the Comptroller's employees on the Core-CT financial team are under the Budget and Financial Analysis Division. The Comptroller's employees on the Core-CT HRMS team are under the Payroll Services Division. The Core-CT technical team is under the OSC Information Technology Division.

Department of Administrative Services

The Department of Administrative Services operates primarily under the provisions of Title 4a, Chapter 57 of the General Statutes. Descriptions of the major functions of the department that are relevant to the Core-CT System are presented below.

The department's responsibilities, which significantly impact the Core-CT System, include: providing statewide human resources services that include the establishment and administration of personnel policies of state employees; the purchase and provision of supplies, materials, equipment and contractual services, as defined in section 4a-51 of the General Statutes; and the purchase and contracting for information systems and telecommunication system facilities, equipment, and services for state agencies, as defined in sections 4d-1 and 4d-2 of the General Statutes.

It should be noted that, effective July 1, 2011, a significant agency reorganization occurred, and DAS absorbed the functions of other agencies. Pursuant to Public Act 11-51, all statutory authority of the former Department of Information Technology was transferred to the Department of Administrative Services – Bureau of Enterprise Systems and Technology. DAS employees on the Core-CT HRMS team are under the DAS Statewide Human Resources Management Division. DAS employees on the Core-CT Financial team are under the DAS Procurement Services Division.

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our examination of the Core-CT System disclosed the following 5 recommendations, of which 3 have been repeated from the previous audit:

Lack of Staffing and Reliance on Consultants

Criteria: Enterprise-level accounting systems such as Core-CT require significant, dedicated, and experienced personnel to better ensure stable operations, system reliability, and the ability to make necessary changes. Although industry best practices do not dictate specific levels, there should be sufficient staffing to ensure continued operational success, attend to reasonable future capacity and capabilities, and promptly respond to unforeseen events.

Condition: Core-CT staffing levels declined in recent years due to resignations and retirements, and significant positions remain vacant. Seven HRMS developer positions are vacant and the HRMS application lead retired during this engagement.

In addition, Core-CT increased its reliance on third-party consultants and vendors, who often perform tasks that would be performed by agency employees.

Effect: Without sufficient staffing, continued operations could be compromised. This could lead to increased unplanned system outages, the inability to add new functionality, and the deferral from planned initiatives to respond to unexpected events. Furthermore, reliance on consultants and vendors could lead to loss of institutional system knowledge, a lack of in-depth familiarity of system changes, and disproportionate trust in vendor abilities.

Cause: Staffing levels have decreased with only limited success in retaining new staff. Although the Financials application team successfully updated its job descriptions, the Human Resources Management System team has not been able to match its job descriptions with the skill sets necessary to hire new staff.

Prior Audit Finding: This finding has not been previously reported.

Recommendation: Core-CT management should ensure sufficient staffing levels to cover current operational needs, reduce reliance on consultants or vendors, and prevent further loss of institutional knowledge through personnel reductions and impending retirements. (See Recommendation 1.)

Agency Response: "Core-CT agrees with this recommendation. Staffing levels need to be addressed. We are also exploring longer term system support options based on the SaaS application delivery model."

Lack of Comprehensive Risk Assessment

Criteria: The National Institute of Standards and Technology (NIST) recommends various risk assessment controls in its Special Publication 800-53 (SP 800-53). Control RA-3, Risk Assessment, requires that the organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, and transmits.

b. Documents the risk assessment results in an organization-defined document.

c. Reviews the risk assessment results at an organization-defined frequency.

d. Disseminates risk assessment results to organization-defined personnel.

e. Updates the risk assessment at an organization-defined frequency or after significant changes to the system, its environment, or other conditions impacting the security of the system.

Condition: While Core-CT conducted some of these best practices, Core-CT management has not completed and documented a formal and comprehensive risk assessment for the Core-CT System.

Effect: Lack of a comprehensive risk assessment could lead to unforeseen events negatively affecting operations.

Cause: It appears that staffing levels and the need to prioritize other aspects of operations contributed to the lack of a risk assessment.

Prior Audit Finding: This finding has not been previously reported.

Recommendation: Core-CT management should conduct and document a full risk assessment, which identifies threats and vulnerabilities, and their likelihood and impact on operations and assets. (See Recommendation 2.)

Agency Response: "Core-CT agrees with this recommendation. Insufficient staffing levels have hindered our ability to complete the risk assessment."

Full Disaster Recovery Test

Criteria: The National Institute of Standards and Technology (NIST) recommends various contingency planning (CP) controls in Special Publication 800-53 (SP 800-53). Control CP-2, Contingency Planning, requires that the organization reviews the contingency plan at an organizational-defined frequency. Additional updates to the contingency plan would address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

Condition: Core-CT has not tested its disaster recovery plan using the full processing demand of all system components.

Effect: Without a complete fail-over and fail-back test, activation of a disaster recovery plan in response to an actual loss of the primary production facility could lead to unnecessary downtime, loss of data, or the inability to restore to the backup site.

Cause: Staffing shortages and budgetary constraints contributed to the inability to complete a full test to successfully transition between the system's main production site and its backup processing site.

Prior Audit Finding: Components of this finding have been previously reported in the last audit report covering general controls as of November 2014.

Recommendation: Core-CT management should conduct a full fail-over and fail-back test cycle to help ensure preparation for a disaster or other significant detrimental event. (See Recommendation 3.)

Agency Response: "Core-CT agrees with this recommendation. Diminishing technical support staffing levels have made it difficult for Core-CT to fully test its disaster recovery processes on an ongoing basis. We do have monitoring processes in place that assure that production data is being successfully replicated to the disaster recovery site 24/7."

Lack of Service-Level Agreement

Criteria: The National Institute on Standards and Technology (NIST) recommends various contingency planning (CP) controls in Special Publication 800-53 (SP 800-53). Control CP-6, Alternate Storage Site, states that an organization should establish an alternate storage site, including any necessary agreements to permit the storage and recovery of information system backup data.

Condition: There is no agreement between the Office of the State Comptroller and the current provider of the Core-CT disaster recovery hot site location.

Effect: Without a defined agreement, Core-CT remains at risk of the provider changing its backup recovery site.

Cause: Core-CT informed us that, during the project's implementation, there was a draft memorandum of understanding regarding the terms of the Comptroller's use of the provider's data center. However, we could not determine why the agreement was never fully executed.

Prior Audit Finding: This finding was previously reported in the last audit report covering general controls as of November 2014.

Recommendation: Core-CT management should enter into a formal agreement for use of the facilities housing the Core-CT disaster recovery hot site. (See Recommendation 4.)

Agency Response: "Core-CT agrees with this recommendation and will pursue a formal agreement. However, since the disaster recovery site is a State facility, the risks highlighted above are diminished."

Lack of Background Checks

Criteria: The National Institute of Standards and Technology (NIST) recommends various personnel security controls (PS) in its special publication 800-53 (SP 800-53).

Control PS-3, Personnel Screening, requires that the organization:

a. Screens individuals prior to authorizing access to the information system.

b. Rescreens individuals according to organizational defined conditions requiring rescreening and the frequency of such rescreening, when applicable.

Condition: We interviewed Office of the State Comptroller personnel responsible for Core-CT staffing and determined that OSC does not perform background checks on newly hired employees who have access to sensitive and classified data.

Effect: Sensitive data and software applications are put at an increased risk of theft, destruction, or alteration.

Cause: Although a specific cause was not identified, it appears that OSC has taken the position that background checks are not required.

Prior Audit Finding: This finding was previously reported in the last audit report covering general controls as of November 2014.

Recommendation: Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT System. (See Recommendation 5.)

Agency Response: "While NIST recommends various personnel security controls, Connecticut General Statutes address the limitations and restrictions of using "background" information—particularly arrest and conviction histories—in state employment decision-making. Core-CT will study the feasibility and legal and practical requirements of requiring background checks."

RECOMMENDATIONS

Our prior audit report on the Core-CT System contained 13 recommendations. Ten have been implemented or otherwise resolved and 3 have been repeated or restated with modifications during the current audit.

Status of Prior Audit Recommendations

- The Core-CT security administration group should take steps to ensure that permission lists are always assigned appropriate sign-on schedules. **The current review found that the permission list errors identified previously have been corrected. This finding has been resolved.**

- The Core-CT security administration group should take steps to ensure that password controls are properly configured in the back-end production databases. **The current review identified an appropriate configuration change to database password controls. This finding has been resolved.**

- Core-CT personnel should strengthen its controls over segregation of duties conflicts within the Core-CT System and develop a means of tracking any exceptions or waivers that they have granted to certain employees or departments. **The current review noted that prior outstanding items were corrected. This finding has been resolved.**

- The Core-CT security administration group should develop procedures to ensure that all database application controls are used where appropriate and configured properly to prevent unauthorized access to confidential information. **Current testing revealed that controls were strengthened in this area. This finding has been resolved.**

- The Core-CT security administration group should develop procedures to ensure a periodic review of who has access the databases behind the Core-CT System and ensure that user accounts are deactivated in a timely manner. **Current testing noted that the previous exceptions were corrected, and current access controls are appropriate. This finding has been resolved.**

- The Core-CT security administration group should develop procedures to ensure a periodic review of what access each database user has and ensure that access levels are appropriate and consistent with the job duties. **Our current review found that access to these accounts is now reviewed monthly, and access is discontinued when no longer necessary. This finding has been resolved.**

- The Core-CT security administration group should develop procedures to ensure that no single database user account, with the exception of system usernames used by database administrators, is shared by more than one individual, and that passwords never match their associated usernames. **Password controls identified as strengthened above also prevent usernames and passwords from matching. This finding has been resolved.**

- The Core-CT security administration group should develop procedures to ensure that no database user account has the same password as the username. **The current audit revealed that the password configuration was adjusted to prevent the use of a password matching a user's ID. This finding has been resolved.**

- The Core-CT security administration group should strengthen controls over migration of code and data from development to production. Errors should be identified during development and testing and should be fixed prior to migration. **Our current review noted that the condition was corrected and has not since reoccurred. This finding has been resolved.**

- Core-CT management should implement application controls relative to assets, where appropriate, upon their upgrade to the new financials system and should develop procedures to ensure that Core-CT asset balances reconcile with associated activity. **The current review noted that asset entry has been modified to ensure asset balances reconcile with their associated activity. This finding has been resolved.**

- Core-CT should develop and completely test a single comprehensive disaster recovery plan for the Core-CT System, with detailed post write-ups to be completed after each test. **Significant progress has been made to address this issue since the prior audit. However, a full and comprehensive test of the disaster recovery plan has not yet been performed. This finding is therefore being repeated in modified form. (See Recommendation 3.)**

- A formal agreement outlining the terms of the Office of the State Comptroller's use of the provider's datacenter as a Core-CT disaster recovery hot site should be written and executed. **Our current review disclosed no change in this condition. This recommendation is being repeated. (See Recommendation 4.)**

- Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT System. **Our current review disclosed no change in this condition. This recommendation is being repeated. (See Recommendation 5.)**

Current Audit Recommendations

1. **Core-CT management should ensure sufficient staffing levels to cover current operational needs, reduce reliance on consultants or vendors, and prevent further loss of institutional knowledge through personnel reductions and impending retirements.**

   Comment:

   Core-CT staffing levels declined in recent years due to resignations and retirements, and significant positions remain vacant. In addition, Core-CT increased its reliance on third-party consultants and vendors, who often perform tasks that would be performed by agency employees.

2. **Core-CT management should conduct and document a full risk assessment, which identifies threats and vulnerabilities, and their likelihood and impact on operations and assets.**

   Comment:

   Core-CT management has not completed and documented a formal and comprehensive risk assessment for the Core-CT System.

3. **Core-CT management should conduct a full fail-over and fail-back test cycle to help ensure preparation for a disaster or other significant detrimental event.**

   Comment:

   Core-CT has not tested its disaster recovery plan using the full processing demand of all system components

4. **Core-CT management should enter into a formal agreement for use of the facilities housing the Core-CT disaster recovery hot site.**

   Comment:

   There is no agreement between the Office of the State Comptroller and the current provider of the Core-CT disaster recovery hot site location.

5. **Core-CT management should develop procedures to ensure that background checks are completed for all employees working on the Core-CT System.**

   Comment:

   We interviewed the Office of the State Comptroller personnel responsible for Core-CT staffing and determined that OSC does not perform background checks on newly hired employees who have access to sensitive and classified data.

ACKNOWLEDGEMENTS

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 State Comptroller and the Department of Administrative Services during the course of our examination.

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

Natercia Freitas
Douglas Stratoudakis
Christopher D'Amico
Crystal Liu

Christopher M. D'Amico
Associate Auditor

Approved:

John C. Geragosian
State Auditor