Office of the Washington State Auditor
Pat McCarthy

Application System Audit Report

ctcLink

Administered by State Board for Community and Technical Colleges

Published August 12, 2024

Report No. 1035361

Scan to see another great way we're helping advance #GoodGovernment

Office of the Washington State Auditor
Pat McCarthy

August 12, 2024

Paul Francis
Board of Directors
State Board for Community and Technical Colleges
Olympia, Washington

Report on Application System Audit

Thank you for the opportunity to work with you to promote accountability, integrity and openness in government. The Office of the Washington State Auditor takes seriously our role of providing state and local governments with assurance and accountability as the independent auditor of public accounts. In this way, we strive to help government work better, cost less, deliver higher value and earn greater public trust.

Independent audits provide essential accountability and transparency for the operations of the State Board for Community and Technical Colleges. This information is valuable to management, the governing body and public stakeholders when assessing the government's stewardship of public resources.

Attached is our independent audit report on the ctcLink system's application and general information technology controls. We appreciate the opportunity to work with your staff and value your cooperation during the audit.

Sincerely,

Pat McCarthy, State Auditor

Olympia, WA

Americans with Disabilities

In accordance with the Americans with Disabilities Act, we will make this document available in alternative formats. For more information, please contact our Office at (564) 999-0950, TDD Relay at (800) 833-6388, or email our webmaster at webmaster@sao.wa.gov.

TABLE OF CONTENTS

AUDIT RESULTS

Results in brief

This report describes the overall results and conclusions for the areas we examined related to the ctcLink system's application, interface and general information technology (IT) controls. In most of the areas we examined, controls were adequately designed and implemented to provide reasonable assurance of complete, accurate, secure and available data.

However, we identified significant deficiencies in the State Board for Community and Technical Colleges' (SBCTC) internal control over IT governance, which we included in this report. We also communicated certain matters related to IT security to SBCTC's management and Board of Directors in a separate confidential finding.

Because public distribution of the tests performed and the related results could increase the risk to SBCTC's IT security, distribution of that information has been limited to management and the Board of Directors, and is kept confidential under RCW 42.56.420.

In keeping with general auditing practices, we did not examine every function or aspect of the application system. Instead, based on our audit objectives, we examined those key application, interface and general IT controls representing the highest risk to the application system's security, availability and processing integrity. Our assessment of controls related to data security was limited to ctcLink. Our audit was not designed to assess or provide assurance on SBCTC's overall security posture.

About the audit

This report contains the results of our independent audit of the ctcLink system. Our audit examined the controls in place from July 1, 2023, through March 31, 2024.

SBCTC coordinates the state's system of 34 public community and technical colleges. In this role, SBCTC is responsible for enterprise resource planning system software that all colleges use for their accounting and financial transactions. Beginning in 2010, SBCTC embarked on a project to replace its legacy financial system with a new one called ctcLink. SBCTC hired a consulting firm to configure and implement the system to fit the business needs of the community and technical colleges. As of May 2022, SBCTC had implemented the ctcLink system at all colleges.

Management is responsible for ensuring IT systems are designed, implemented and maintained to provide reasonable assurance of security, availability and processing integrity. This includes establishing controls over acquiring, developing and maintaining technology assets relevant to these objectives.

This audit was conducted under the authority of RCW 43.09.310, which requires the Office of the Washington State Auditor to examine the financial affairs of all state agencies. Our audit involved obtaining evidence about the ctcLink system's key application and interface controls, along with related general IT controls. The procedures we performed were based on our assessment of risks in the areas we examined.

Based on our risk assessment, we examined the following areas during this audit period:

- **IT governance controls** related to disaster recovery and business continuity planning, fraud, end-user training, and third-party monitoring. System governance controls include management oversight of the ctcLink system and responsibilities of its use. These controls are designed to ensure the effective management and oversight of the system and its continued functionality.
- **General IT controls** related to user access. General IT controls are designed to ensure proper development, integrity and security of system and computer operations.

SCHEDULE OF AUDIT FINDINGS AND RESPONSES

State Board for Community and Technical Colleges
July 1, 2023 through March 31, 2024

2024-001 The State Board for Community and Technical Colleges did not have adequate internal controls over information technology governance of ctcLink.

Background

The State Board for Community and Technical Colleges (SBCTC) provides oversight and administrative support for all 34 community and technical colleges in Washington. SBCTC supports a common enterprise resource planning (ERP) system for all colleges to use. In August 2015, SBCTC released a new ERP system, ctcLink, at two colleges. SBCTC did not complete the implementation of the new system for the remaining colleges until May 2022, largely because of initial system functionality concerns and issues identified early in the implementation process.

SBCTC is responsible for information technology (IT) governance and ownership of ctcLink because it provides the system all 34 colleges are required to use. The colleges are responsible for their individual business processes as they facilitate student registration, course management, payroll, human resources, financial aid, and financial services for their students and employees. The colleges and SBCTC share the responsibility of data that is held and processed within ctcLink.

In the 2018 and 2022 audits, we recommended SBCTC improve or implement the functionality and transaction controls over ctcLink. The scope of the current audit of ctcLink was to determine whether SBCTC's internal controls over IT governance were adequate in providing effective oversight of the system.

Description of Condition

Due to deficiencies in internal controls over IT governance that have existed since ctcLink's initial launch in 2015, SBCTC has not adequately assessed or communicated the system's risks that have led to known or potential issues for the colleges.

Disaster Recovery and Business Continuity Planning

SBCTC did not consider critical resources or information systems that support the continued functionality of ctcLink within its disaster recovery and business continuity plans. Additionally, SBCTC did not consider the effect that losing such critical resources or information systems would have on the agency or the colleges that rely on the functionality of ctcLink for uninterrupted business operations.

Fraud Controls

SBCTC did not implement automated fraud-prevention and detection controls over student aid within ctcLink. SBCTC did not adequately assess the risk of not having these automated controls nor the operational and financial effect frauds would have on colleges.

End-User Training

SBCTC lacked effective internal controls to ensure that ctcLink's end users were properly trained, and did not assume ownership of ctcLink's end-user training program. SBCTC did not adequately assess the risk of inaccurate data to the statewide and college reporting requirements.

Third-Party Monitoring

State law (RCW 39.26.340) requires state agencies that share confidential information with contractors to establish written data-sharing agreements. SBCTC did not ensure its agreements with contractors that have access to confidential information contained all elements required by the State Office of Cybersecurity.

Cause of Condition

Disaster Recovery and Business Continuity Planning

SBCTC did not dedicate resources to evaluating the business operation effect on all the colleges and more than 250,000 students if ctcLink were to become nonoperational due to the loss of a critical supporting resource. Since 2015, SBCTC focused its resources on correcting functional system errors and implementing ctcLink at all colleges.

Fraud Controls

While SBCTC currently conducts a risk assessment over ctcLink, it did not adequately evaluate the risks associated with not having automated fraud-prevention and detection controls over student aid within the system. SBCTC

did not actively collaborate with the colleges to discuss uniform fraud-prevention and detection controls over student aid until after the last college converted to ctcLink in 2022.

End-User Training

SBCTC developed training resources for end users, but it delegated the responsibility of training requirements and tracking to each college after it went live with ctcLink. College employees are the end users, but the transactional data being captured, processed and held within ctcLink are used at both the college and statewide levels, which makes the accuracy of the information the joint responsibility of both SBCTC and the colleges.

Third-Party Monitoring

SBCTC officials thought the language included in the agreements with contractors addressed all the elements for data-sharing agreements required by state law and the standards prescribed by the State Office of Cybersecurity. However, our audit confirmed the current language did not address all required elements.

Effect of Condition

SBCTC's lack of effective internal controls and oversight of ctcLink increases the risk that it would not be able to prevent, detect or remediate misappropriation, misuse, fraud or prolonged system disruption in a timely manner.

Disaster Recovery and Business Continuity Planning

Because SBCTC lacks a comprehensive disaster recovery plan that considers all resources that support the ongoing functionality of ctcLink, it cannot effectively demonstrate to all colleges the overall effect or remediation efforts needed in the event of a system disruption or other disaster.

Fraud Controls

Since ctcLink does not have automated fraud-prevention and detection controls over student aid – and SBCTC did not adequately evaluate the risks associated with not implementing these controls – Washington's community and technical colleges have a higher risk of student aid fraud. Since 2022, our Office has received seven loss reports across six colleges totaling more than $85,000.

End-User Training

In our 2023 audit of the state's Annual Comprehensive Financial Report, SBCTC received multiple recommendations that were partly attributed to college employees' lack of knowledge of how to properly process financial transactions within ctcLink.

Third-Party Monitoring

SBCTC did not have all the elements required by the State Office of Cybersecurity in its data-sharing agreements with two of its contractors that have access to confidential information, resulting in noncompliance with state law (RCW 39.26.340). By leaving out required elements in its agreements with contractors, SBCTC increases its risk of confidential information being mishandled or compromised.

Recommendation

We recommend SBCTC implement adequate internal controls over IT governance of ctcLink to increase assurance of the system's reliability and functionality to the colleges and students in Washington.

We also recommend SBCTC ensure compliance with applicable regulatory requirements, internal and external policy requirements, and best practices. Specifically, we recommend SBCTC:

Disaster Recovery and Business Continuity Planning

- Identify and document all critical resources and information systems that support the continued functionality of the ctcLink system within SBCTC's disaster recovery and business continuity plans. This includes analyzing the potential effect that a loss of these critical supporting resources or information systems would have on SBCTC, the colleges, and the students they serve.

Fraud Controls

- Assess, evaluate, and document the risk and effect of not having system-based fraud-prevention and detection controls to verify, or assist in verifying, student applicants' identities before they receive financial aid

End-User Training

- Develop stronger controls over the accuracy of statewide transactional data by reevaluating the end-user training requirements. This would include assessing, evaluating and documenting the risks and effects of not requiring end users to participate in required trainings and not having a control mechanism to actively monitor or track training participation

Third-Party Monitoring

- Implement data-sharing agreements that include all the elements required by state law and the standards prescribed by the State Office of Cybersecurity

Agency's Response

Disaster Recovery and Business Continuity Planning

SBCTC is acutely aware of the significant disruption that any downtime of the ctcLink application could cause to colleges and their students and has proactively implemented a PeopleSoft (PS) backup solution. This backup system is designed to ensure a swift recovery time of approximately 10 minutes for all databases, with the capability to restore data to any point within the past 30 days. Additionally, daily backups are maintained for further security and data integrity.

For third-party applications such as the Online Admissions Application Portal (OAAP), SBCTC has taken significant steps to ensure continuity and rapid recovery in the event of system failure and has implemented a robust daily recovery protocol. This system retains backups for an entire year and facilitates the restoration of services to a new server within a mere 30 minutes, should the need arise. This strategy not only secures the data on a day-to-day basis but also allows for a comprehensive archival of information spanning a year.

This swift restoration capability is crucial during peak admissions periods when any amount of downtime could have severe repercussions on enrollment processes.

Moreover, SBCTC's approach includes regular testing of the backup and restoration procedures for OAAP to ensure that, if required, the process will run smoothly and efficiently. The testing protocols also help identify potential issues or bottlenecks that could delay recovery times, allowing for preemptive measures to be taken.

In addition to these technical measures, SBCTC has developed a comprehensive communication plan to promptly inform all stakeholders, including college administrators, staff, and prospective students, in the event of an OAAP system disruption. This ensures transparency and allows for alternative arrangements to be made swiftly; thereby minimizing inconvenience and maintaining the integrity of the admissions process.

Overall, the disaster recovery and business continuity plans reflect SBCTC's dedication to providing resilient and reliable services that support the critical functions of community and technical colleges in Washington state.

Fraud Controls

Comprehensive efforts have been taken to address documentation and collaboration efforts regarding preventative and detection controls for the system. We are committed to continued collaboration and acknowledge the importance of implementing effective internal controls to assist colleges in mitigating this risk.

As early as mid-2020, we developed a system service indicator to identify fraudulent accounts. Following that, in early 2021, a quick reference guide (QRG) was created for colleges to identify fraudulent student accounts and verify legitimate ones. The SBCTC IT division has consistently evaluated and updated this documentation as the student fraud landscape has evolved. In early 2023, a service indicator synchronization job process was created to disburse the fraudulent account service indicator across all colleges. This process aided in the prevention of subsequent enrollments and financial aid disbursements until the account was verified as a non-fraudulent account.

In April 2023, SBCTC collaborated with the Education and Business Operations divisions to issue a memorandum to the colleges on mitigating enrollment and student financial fraud. This memorandum included guidance on reporting requirements to SBCTC, Office of the Washington State Auditor, and the U.S. Department of Education. Additionally, SBCTC updated the quick reference guide to incorporate new system-wide service indicators and reports available in ctcLink, aiding colleges in detecting, documenting, and preventing fraudulent activity.

In mid-2023, SBCTC IT formed a fraudulent application subgroup with members from the college community. This subgroup was established to explore additional opportunities for creating system-wide fraud prevention and detection controls within ctcLink. The group is focused on developing a global business process for detecting, identifying, and preventing fraudulent student accounts across all colleges. Another focus of the subgroup is the admissions process into ctcLink. SBCTC is collaborating with our vendor partner to provide automated security

controls. Of the few items under SBCTC purview, these controls aim to meet the components of the Department of Education's GEN 11-17, such as: identifying IP addresses, utilization of email addresses across the system, and being able to prevent aid disbursements until validation of identity.

Most recently, in April 2024, the fraudulent application subgroup transitioned to the purview of the systemwide Admissions and Registration Council (ARC), comprised of college enrollment staff and leadership. The SBCTC will continue to participate in ongoing discussions and collaboration with the community and technical colleges to mitigate fraudulent activity. SBCTC remains committed to documenting the risks associated with not having a unified business process across all institutions and ctcLink to combat these types of fraud activities effectively.

End User Training

As part of our continuous improvement efforts during the project implementation, and as we transitioned into long-term stabilization and maintenance of the ctcLink system, our training team has consistently evolved and updated multiple training resources for the colleges. Over the past several years, the training team has created approximately 80 Canvas training courses, over 7,000 quick reference guides, and has conducted numerous instructor-led training courses for the colleges.

Recently, the training team developed and delivered modular onboarding manuals for college use. Alongside these onboarding materials, the team released an online training application that allows all end users and supervisors to track the progress and completion of ctcLink training courses in which each staff member has engaged across all 34 community and technical colleges.

In addition, the Business Operations division has created and implemented a Controller Handbook to provide the colleges with standardized accounting practices across all colleges.

In addition to knowing how to use ctcLink software, colleges also wanted learning opportunities about how to perform specific fiscal-related processes. To that end, the SBCTC Business Operations ctcLink Accounting Team developed a robust set of offerings for accounting and student financials staff. (See a recent ctcLink CONNECT blog "Finance (FIN) News" section for detailed session information: https://www.sbctc.edu/blogs/ctclink-connect/2024/2024-05-08)

Highlight of offerings:

- *Chartstring Clean-Up Working sessions & Special Topics (weekly) are hands-on sessions to help colleges get ready for the transition from AFRS to OneWA.*
- *Fiscal Year-end Work Sessions (daily except holidays) are focused work sessions for accounting support and guidance with topics including FYE preparation, reconciliation, and processes.*
- *Finance College Users Production Support meetings (weekly) provide updates on service tickets, PeopleSoft enhancements, and open forum time to ask questions or request future topics.*
- *Student Finance/General Ledger SF/GL Open Forums (monthly) cover everything from item types and second journal sets to waivers, queries, or internal cash reconciliation.*
- *Grants/Projects Q&A Drop-In (monthly) offer collaborative and interactive troubleshooting on everything Grants/Projects-related.*

Moving forward, in alignment with the provided recommendations, the SBCTC training team aims to enhance control opportunities related to the requirement of end-user training. The SBCTC, in collaboration with the colleges, will work to ensure the accuracy of information in ctcLink is based on relevant training, ensuring consistency for all users.

Third Party Monitoring

While many of the protections required in data sharing agreements are already covered by SBCTC contracts, we recognize the need for more specificity and attention to areas of concern when it comes to data sharing specifically.

We are actively working to develop a specific "Data Sharing" section or exhibit to add to contracts, so our data sharing covers any areas of need in greater detail.

We are using the Office of the Chief Information Officer's "Data Sharing Agreement Implementation Guidance" document to help focus these efforts. Our new language should be in place in time to be used in all contracts with Data Sharing components by July 1, 2024.

Auditor's Remarks

We thank SBCTC for its cooperation and assistance during the audit. We have evaluated SBCTC's responses, and we reaffirm our finding that SBCTC did not have adequate internal controls over IT governance of ctcLink.

Applicable Laws and Regulations

Disaster Recovery and Business Continuity Planning

Washington Technology Solutions policy SEC–12, *"INFORMATION TECHNOLOGY DISASTER RECOVERY PLANNING POLICY,"* states in part:

1. Agencies must develop Information Technology (IT) Disaster Recovery (DR) plan(s) in support of the agency Continuity of Operations Plan (COOP), including services, and applications reported as mission critical and business essential.

    a. DR plan(s) are required for each technology necessary to support and deliver the agency's essential functions documented in the agency's COOP.
    b. DR plan(s) must include, document, and account for interdependencies with:

        i. Roles critical for executing the plan(s).
        ii. Other systems.
        iii. Internal or externally hosted applications.
        iv. Inter-agency service providers, such as WaTech, DES, or OFM.
        v. External parties such as public cloud providers, Software as a Service (SaaS) solutions, and data storage

    c. DR plan(s) must be reviewed, updated, and exercised at least every other year.

        i. Within 90 days of the production date, agencies must review, update, and exercise plans for new applications or services or those that undergo significant changes or major upgrades.
        ii. Agencies must document objectives of the exercise.
        iii. Agencies must document exercise results.
        iv. Agencies must identify and document corrective actions and/or risk mitigations based on exercise results and update the DR plan accordingly.
        v. Agencies must demonstrate in their documentation that service providers or other external parties that support critical services or essential functions comply with annual exercise requirements.

2. Agencies must ensure employees, contractors, and external parties are engaged in exercises and/or complete training as to their role in executing the agency's DR Plan(s).
3. Agency heads are responsible for ensuring compliance with this policy and must approve the annual DR plan(s).

RCW 38.52.030 states in part:

> (11) The director is responsible to the governor to lead the development and management of a program for interagency coordination and prioritization of continuity of operations planning by state agencies. Each state agency is responsible for developing an organizational continuity of operations plan that is updated and exercised annually in compliance with the program for interagency coordination of continuity of operations planning.

State Board for Community and Technical Colleges Cyber Security Standardized Operating Procedures (CSOP); P-RA-9: "*CRITICALITY ANALYSIS*"

Fraud Controls

U.S. Department of Education GEN-11-17 states in part:

- Implement automated protocols that monitor information in your student information data system to identify instances where a number of students –
    - Use the same Internet Protocol (IP) address to complete and submit an admissions application.
    - Use the same IP address to participate in the on-line academic program.
    - Use the same e-mail address to submit an admissions application.
    - Use the same e-mail address to participate in the on-line academic program.
    - Appear to reside in a geographic location that is anomalous to the locations of most students in the program.
- Modify your disbursement rules for students participating exclusively in distance learning programs, which would immediately reduce the amount that fraud ring participants can receive. Institutions have the authority to:
    - Delay disbursement of Title IV funds until the student has participated in the distance education program for a longer and more substantiated period of time (e.g., until an exam has been given, completed, and graded or a paper has been submitted).

- Make more frequent disbursements of Title IV funds so that not all of the payment period's award is disbursed at the beginning of the period.

National Institute of Standards and Technology Special Publication 800-63A "*Digital Identity Guidelines – Enrollment and Identity Proofing Requirements*"

End-User Training

National Institute of Standards and Technology Special Publication NIST 800-12 "*An Introduction to Information Security*" – Chapter 10.2 "*Awareness & Training,*" Chapter 4.2.1 "*Errors and Omissions,*" and Chapter 5.2.1 "*Basic Components of Program Policy*"

Third-Party Monitoring

RCW 43.105.205 states in part:

> (3) In the case of institutions of higher education, the powers of the office and the provisions of this chapter apply to business and administrative applications but do not apply to (a) academic and research applications; and (b) medical, clinical, and health care applications, including the business and administrative applications for such operations.

RCW 39.26.340 states in part:

> (1) Before an agency shares with a contractor category 3 or higher data, as defined in policy established in accordance with RCW 43.105.054, a written data-sharing agreement must be in place. Such agreements shall conform to the policies for data sharing specified by the office of cyber security under the authority of RCW 43.105.054.

Washington Technology Solutions policy SEC–08, *"DATA SHARING POLICY,"* states in part:

1. Agencies must enter into written data sharing agreements when sharing category 3 or category 4 data outside the agency unless otherwise prescribed by law.
2. Agencies must identify and evaluate the risks of sharing their data and must enter into a data sharing agreement that documents the relationship and includes appropriate terms to mitigate identified risks.
3. Data sharing agreements can take different forms but should typically include at least:

a. The purpose and specific authority for sharing and time period of the agreement.
b. A description of the data, including classification.
c. Period of agreement.
d. Authorized uses.
e. Authorized users or classes of users.
f. Protection of the data in transit if the arrangement involves transmission. See SEC08-02-S Encryption Standard.
g. Secure storage for data maintained outside the agency sharing its data.
h. Data retention and disposal responsibilities and processes.
i. Backup requirements for the data if applicable.
j. Incident notification and response.
k. Monitoring and enforcement of data protection requirements specified in the agreement.
l. All parties must have a security awareness program and/or training.
m. Compliance with all relevant state security and privacy requirements associated with the data being shared.
n. Any other requirements imposed by law, regulation, contract, or policy.

ABOUT THE STATE AUDITOR'S OFFICE

The State Auditor's Office is established in the Washington State Constitution and is part of the executive branch of state government. The State Auditor is elected by the people of Washington and serves four-year terms.

We work with state agencies, local governments and the public to achieve our vision of increasing trust in government by helping governments work better and deliver higher value.

In fulfilling our mission to provide citizens with independent and transparent examinations of how state and local governments use public funds, we hold ourselves to those same standards by continually improving our audit quality and operational efficiency, and by developing highly engaged and committed employees.

As an agency, the State Auditor's Office has the independence necessary to objectively perform audits, attestation engagements and investigations. Our work is designed to comply with professional standards as well as to satisfy the requirements of federal, state and local laws. The Office also has an extensive quality control program and undergoes regular external peer review to ensure our work meets the highest possible standards of accuracy, objectivity and clarity.

Our audits look at financial information and compliance with federal, state and local laws for all local governments, including schools, and all state agencies, including institutions of higher education. In addition, we conduct performance audits and cybersecurity audits of state agencies and local governments, as well as state whistleblower, fraud and citizen hotline investigations.

The results of our work are available to everyone through the more than 2,000 reports we publish each year on our website, www.sao.wa.gov. Additionally, we share regular news and other information via an email subscription service and social media channels.

We take our role as partners in accountability seriously. The Office provides training and technical assistance to governments both directly and through partnerships with other governmental support organizations.

Stay connected at sao.wa.gov

- Find your audit team
- Request public records
- Search BARS Manuals (GAAP and cash), and find reporting templates
- Learn about our training workshops and on-demand videos
- Discover which governments serve you — enter an address on our map
- Explore public financial data with the Financial Intelligence Tool

Other ways to stay in touch

- Main telephone: (564) 999-0950
- Toll-free Citizen Hotline: (866) 902-3900
- Email: webmaster@sao.wa.gov