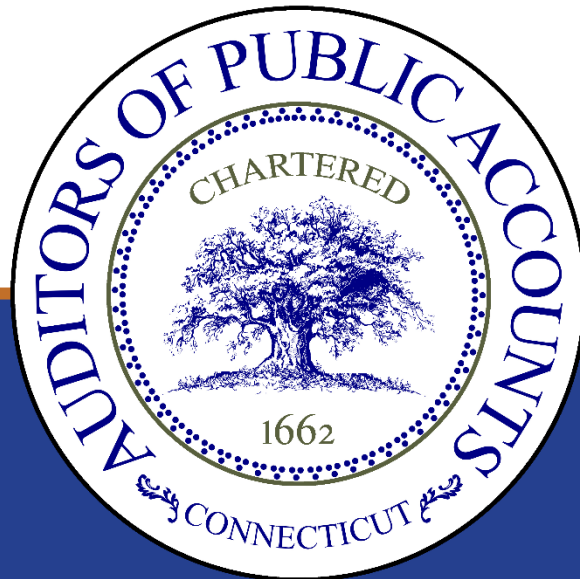


AUDITORS' REPORT

CONNECTICUT STATE
COLLEGES AND UNIVERSITIES
SYSTEM OFFICE

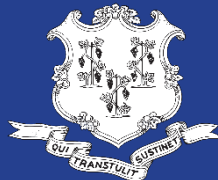
Banner Information System

AS OF NOVEMBER 2023



STATE OF CONNECTICUT
Auditors of Public Accounts

JOHN C. GERAGOSIAN
State Auditor



CRAIG A. MINER
State Auditor

CONTENTS

INTRODUCTION.....	3
AUDIT-AT-A-GLANCE	4
STATE AUDITORS' FINDINGS AND RECOMMENDATIONS.....	5
Information Technology Policy Deficiency (Planning)	5
OBJECTIVES, SCOPE, AND METHODOLOGY	7
ABOUT THE AGENCY	8

STATE OF CONNECTICUT



AUDITORS OF PUBLIC ACCOUNTS

JOHN C. GERAGOSIAN

STATE CAPITOL
210 CAPITOL AVENUE
HARTFORD, CONNECTICUT 06106-1559

CRAIG A. MINER

July 2, 2024

INTRODUCTION

We are pleased to submit this audit of the Connecticut State Colleges and Universities (CSCU) System Office's Banner Information System as of November 2023 in accordance with the provisions of Section 2-90 of the Connecticut General Statutes. Our audit identified one finding involving an internal control deficiency and an instance of noncompliance with policies or procedures.

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

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

Christopher D'Amico
Jared Kolomyjec
Joan Main

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

Christopher D'Amico
Principal Auditor

Approved:




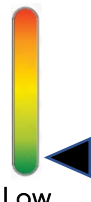
A handwritten signature in black ink, appearing to read "John C. Geragosian".

John C. Geragosian
State Auditor

A handwritten signature in black ink, appearing to read "Craig A. Miner".

Craig A. Miner
State Auditor

AUDIT-AT-A-GLANCE

Category	Audit Risk	Description
Maintenance	 Low	Maintenance controls concern how well organizations keep their information technology (IT) systems up to date, patched, and operational. This engagement did not note any related findings or recommendations.
Personnel	 Low	Personnel controls identify how well the CSCU System Office's IT group is staffed, aware of its responsibilities, and able to perform its duties. This engagement did not note any related findings or recommendations.
Planning	 Moderate	Planning controls indicate how well IT systems are insulated from disruptions, unauthorized access, and similar activities that might detrimentally impact operations. The CSCU System Office should strengthen internal controls to ensure its information technology policies remain current. (Finding 1)
Security	 Low	Security controls identify how well the IT systems are protected (physically and logically) and ensure the office's data are backed up and accessible. This engagement did not note any related findings or recommendations.

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our examination of the information technology general controls of the Connecticut State Colleges and Universities System Office's Banner Information System disclosed the following recommendation, which was not repeated from the previous audit:

Finding 1

Information Technology Policy Deficiency (Planning)

Criteria

The Connecticut State Colleges and Universities System Office's information security policy requires an annual review of policies and procedures, consistent with industry best practices. Furthermore, the office's information security policy relies on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 for authoritative guidance. The most recent NIST SP 800-53 revision (revision 5) was released in September 2020.

Condition

The Connecticut State Colleges and Universities System Office did not update its policies in accordance with its information security policy. The policies we reviewed during the audit were at least two years out of date. Neither the office's information security policy nor its detailed procedures incorporated the NIST SP 800-53 revision 5 update.

Context

Information technology policies provide the foundation for the roles and responsibilities of information technology staff, as well as compliance for all employees. Missing or outdated policies increase the risk of inadequate or incomplete procedures (electronic or human), and undermine efforts to ensure appropriate confidentiality, integrity, and availability of data.

Effect

Outdated policies may include incorrect or incomplete information related to emerging technologies and regulations. As a result, the organization is exposed to greater risk.

Cause

The office has not updated policies due to changes in personnel and shifting management priorities.

Prior Audit Finding

This finding has not been previously reported.

Recommendation

The Connecticut State Colleges and Universities System Office should strengthen internal controls to ensure its information technology policies remain current.

Agency Response

"We agree with this finding. Policies play a critical role in shaping the security practices within CSCU, and we recognize the importance of keeping them current to address emerging technologies and regulatory changes. Changes in personnel and resource limitations have resulted in challenges to conducting a timelier review of our policies. The Information Security Program Office (ISPO) is currently reviewing some of the identified documents, with others planned for review early next year."

OBJECTIVES, SCOPE, AND METHODOLOGY

We have audited certain operations of the Connecticut State Colleges and Universities System Office's Banner Information System in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. The scope of our audit included information technology general controls as of November 2023. The objectives of our audit were to evaluate the:

1. Office's internal controls over the Banner Information System;
2. Office's compliance with policies and procedures internal to the office or promulgated by other state agencies; and
3. Effectiveness 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. This 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 state information systems, and was not subject to the procedures applied in our audit of the office's Banner Information System. For the areas audited, we:

1. Identified a deficiency in internal controls;
2. Identified apparent noncompliance with policies or procedures; and
3. Identified 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 Banner Information System.

ABOUT THE AUDIT

Audit Purpose

We conducted this audit to obtain an understanding of Banner and how it uses and protects the data it maintains. Our review was intended to: (1) identify the design and implementation of 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 Banner Information System's IT control environment.

Audit Overview

The [Connecticut State Colleges and Universities](#) System Office provides oversight to the state's twelve community colleges, four state universities, and the online Charter Oak State College. The office is overseen by the CSCU Chancellor, who is responsible for the day-to-day administration and operation of this organization. It is governed by the Board of Regents for Higher Education.

The Office of Information Technology oversees all aspects of the system office's information technology needs, including enterprise support and infrastructure, local administration of the Banner system, and coordinating related needs across constituent schools.

The Banner Information System represents a significant investment for the state and many of its institutions of higher learning. Designed by Ellucian, Banner is an enterprise higher education resource planning system. Banner collects, processes, and transacts the colleges' and universities' financial, human resource, and student record information.