



Minnesota
STATE COLLEGES
& UNIVERSITIES

Members of the Minnesota State Colleges and Universities Board of Trustees
James McCormick, Chancellor

We have audited internal controls and legal compliance provisions over certain financial activities of St. Cloud Technical and Community College. The audited activities included security over access to computerized accounting applications, banking, employee payroll, operating and administrative expenses (purchased services, employee expense reimbursements, and credit card purchases), equipment purchases, inventory, and capital project spending for fiscal years 2008, 2009 and 2010, through December 31, 2009. We conducted the audit in compliance with the *Institute of Internal Auditors: Standards for Professional Practice of Internal Auditing*.

Audit Objectives and Methodology

Our audit objectives were to determine:

- If internal controls at the college were adequate to ensure the college safeguarded assets, accurately paid employees and vendors in accordance with management's authorization, produced reliable information, and complied with finance-related legal requirements.
- For the items tested, if the college complied with significant finance-related legal requirements over financial activities, including state laws, regulations, contracts, and applicable policies and procedures.

We conducted fieldwork for the audit during June and July 2010. Our testing included:

- Conducting interviews of key staff to gain an understanding of the controls related to financial operations.
- Considering the risks of errors in the accounting records and potential noncompliance with finance-related legal requirements.
- Analyzing accounting data to identify unusual transactions or significant changes in financial operations for further review.
- Selecting a sample of financial transactions and reviewing supporting documentation to test whether the colleges' controls were effective and if the transactions complied with laws, regulations, policies and grant and contract provisions.

Conclusions

The college generally had adequate internal controls over major financial activities such as employee salaries and operating expenses. These controls generally ensured that the college safeguarded assets, accurately paid employees and vendors in accordance with management's authorization, produced reliable financial information, and complied with finance-related legal requirements. However, we noted control weaknesses over computer security access to financial systems and management of equipment. For items tested, the college generally complied with MnSCU policies and finance-related legal provisions. However, the college did not comply with a requirement related to credit card purchases. The identified issues are in areas that have had a high risk of errors and are discussed in more detail in the attached Summary of Findings. In addition, we have communicated other operational issues to management for consideration.

Beth Buse, CPA, CIA, CISA, GSEC
Executive Director, Office of Internal Auditing

September 14, 2010

Summary of Findings

Finding 1: The college did not design, document or monitor detective controls to mitigate risk created by giving an employee incompatible access and unnecessary access to computer systems.

The college provided incompatible security roles for one employee in the Integrated Statewide Record System without defining, documenting, or monitoring the effectiveness of a mitigating control. Separation of duties is necessary for strong internal controls and is a preventative control to prevent the occurrence of errors or fraud. When duties cannot be separated, the college faces an increased risk that errors or irregularities may occur. To mitigate the risk, the college needs to develop detective controls to detect whether errors or irregularities have occurred.

In addition, the college failed to remove security rights for two employees after they left employment with the college. Finally, the college provided security rights to five employees that were not necessary to perform their job responsibilities.

Recommendation

The college should eliminate its incompatible security role or establish and document detective controls to mitigate risks from providing incompatible access. In addition, the college should remove unnecessary security roles that are not based on job responsibilities and ensure that it removes security for employees upon terminating employment.

Finding 2: The college did not adequately manage disposal of equipment and sensitive asset inventory.

Asset disposals were not always communicated to the Business Office and recorded in the equipment module timely. For example, an academic department failed to notify the Business Office that a vehicle had been used and destroyed in a test. In addition, signatures were not always obtained from the department disposing of fixed assets to substantiate the disposal of the asset. Finally, documentation did not always indicate whether the item was removed from the inventory system because it was missing or if it had been properly disposed. By not formally documenting asset disposals and promptly communicating them to the Business Office, the college increases the risk of assets being misappropriated without detection or otherwise being disposed of properly.

Recommendation

The college should review the asset disposal policy with department heads. The college should obtain a signature on the asset disposal form from the department that maintained the asset. In addition, the Business Office should follow up on any assets determined missing from physical inventories to ensure assets were disposed of properly and with the department heads' knowledge.

Finding 3: The college did not sufficiently control employees' use of college-issued credit cards.

The college did not always require original receipts to substantiate payments made by credit cards. For example, we noted instances where some employees had submitted reservations and itineraries for lodging, airfare and car rental to document their expenses rather than original receipts. Confirmations, itineraries and reservation documents do not prove the employee actually incurred the expense. MnSCU Procedure 7.3.3 Part 7 requires cardholders to obtain and retain original itemized receipts for all purchases.

In addition, the college had not implemented merchant category blocking on their college credit cards as required by MnSCU Procedure 7.3.3. Category blocking helps ensure the credit cards are not used at inappropriate merchants. The college implemented category blocking in June 2010.

Recommendation

The college should ensure original receipts are obtained to substantiate credit card payments.

September 13, 2010

Ms. Beth Buse
Office of Internal Audit
350 Wells Fargo Place
30 East Seventh Street
St. Paul, MN 55101

Dear Ms. Buse:

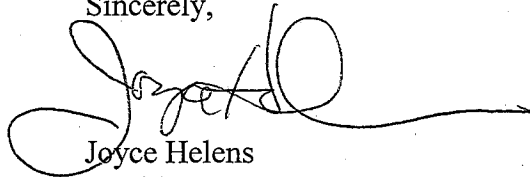
Thank you for the opportunity to respond to the recommendations made in the recently conducted audit at St. Cloud Technical and Community College for fiscal years 2008, 2009, and 2010, through December 31, 2009.

St. Cloud Technical & Community College administration, faculty and staff have committed to a culture of continuous quality improvement. The work completed by your staff has provided the college with continuing assurance that internal control procedures are in place and the college generally complied with MnSCU policies and finance-related legal provisions. The College would like to acknowledge the value of this audit and extend appreciation to the Office of Internal Audit staff for their recommendations to enhance and improve existing internal controls and operations for continuous quality improvement.

In reviewing the audit's findings, we were pleased to note that these were not systemic issues. We agree that additional steps should be taken to tighten controls and further enhance systems to protect and safeguard college assets.

Please find attached the college's responses to the audit findings.

Sincerely,


Joyce Helens
President

**St. Cloud Technical and Community College Response to the Office of Internal Auditing
Internal Control and Legal Compliance Audit
Summary of Findings**

Finding 1: The college did not design, document or monitor detective controls to mitigate risk created by giving an employee incompatible access and unnecessary access to computer systems.

Recommendation:

The college should eliminate its incompatible security role or establish and document detective controls to mitigate risks from providing incompatible access. In addition, the college should remove unnecessary security roles that are not based on job responsibilities and ensure that it removes security for employees upon terminating employment.

Response: The college removed the incompatible security role for one employee and unnecessary security rights for the other employees as recommended. The college appreciates the recent enhancements to the ISRS web based security module and anticipates that the web based efficiencies provided for identification and resolution of unnecessary or incompatible duties will diminish the risk of future security issue occurrences.

Finding 2: The college did not adequately manage disposal of equipment and sensitive asset inventory.

Recommendation:

The college should review the asset disposal policy with department heads. The college should obtain a signature on the asset disposal form from the department that maintained the asset. In addition, the Business Office should follow up on any assets determined missing from physical inventories to ensure assets were disposed of properly and with the department heads' knowledge.

Response: College meetings have been held with all departments reviewing and reinforcing the need for proper signatures on the asset disposal form. Continued communication will take place regarding the proper completion and submission of the asset disposal form. In addition, the college will continue to follow up on assets missing from physical inventory and will document follow up discussions and resolution to the proper disposal of such inventory.

Finding 3: The college did not sufficiently control employees' use of college-issued credit cards.

Recommendation:

The college should ensure original receipts are obtained to substantiate credit card payments.

Response: Travel reimbursement procedures will be clarified with all employees and SCTCC will not process future expense reimbursements without original receipts that document and support actual expenses or, per the travel policy, a notarized affidavit stating that the original receipt was lost or had not been obtained.