OFFICE OF AUDITOR OF STATE
STATE OF IOWA

David A. Vaudt, CPA
Auditor of State

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834 Facsimile (515) 242-6134

NEWS RELEASE

FOR RELEASE October 17, 2008

Contact: Andy Nielsen
515/281-5834

Auditor of State David A. Vaudt today released a report on a review of selected general and application controls over the University of Northern Iowa's tuition and fees system for the period May 24, 2007 through July 3, 2007.

Vaudt recommended the University strengthen password controls, log and review security profile changes, perform comprehensive background checks for new ITS employees, periodically review access rights, implement written procedures for review of system software changes and update and test the contingency plan. Additionally, Vaudt recommended the University establish policies and procedures to conduct periodic risk assessments, to verify mandatory fees are assessed at approved rates, to control access to production programs and for authorization and support for manual billing adjustments.

A copy of the report is available for review at the University of Northern Iowa, in the Office of Auditor of State and on the Auditor of State's web site at http://auditor.iowa.gov/reports/reports.htm.

###

REPORT OF RECOMMENDATIONS TO THE UNIVERSITY OF NORTHERN IOWA ON A REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE TUITION AND FEES SYSTEM

MAY 24, 2007 through JULY 3, 2007

Office of

AUDITOR OF STATE

State Capitol Building • Des Moines, Iowa

David A. Vaudt, CPA
Auditor of State

OFFICE OF AUDITOR OF STATE
STATE OF IOWA

David A. Vaudt, CPA
Auditor of State

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834 Facsimile (515) 242-6134

June 26, 2008

To the Members of the
Board of Regents, State of Iowa:

In conjunction with our audit of the financial statements of the University of Northern Iowa for the year ended June 30, 2007, we conducted an information technology review of selected general and application controls for the period May 24, 2007 through July 3, 2007. Our review focused on the general and application controls of the University's tuition and fees system as they relate to our audit of the financial statements. The review was more limited than would be necessary to give an opinion on internal controls. Accordingly, we do not express an opinion on internal controls or ensure all deficiencies in internal controls are disclosed.

In conducting our review, we became aware of certain aspects concerning information technology controls for which we believe corrective action is necessary. As a result, we have developed recommendations which are reported on the following pages. We believe you should be aware of these recommendations which pertain to the University's general and application controls over the tuition and fees system. These recommendations have been discussed with University personnel and their responses to these recommendations are included in this report.

This report, a public record by law, is intended solely for the information and use of the officials and employees of the University of Northern Iowa, citizens of the State of Iowa and other parties to whom the University of Northern Iowa may report. This report is not intended to be and should not be used by anyone other than these specified parties.

We would like to acknowledge the many courtesies and assistance extended to us by personnel of the University during the course of our review. Should you have any questions concerning any of the above matters, we shall be pleased to discuss them with you at your convenience. Individuals who participated in our review are listed on page 10 and they are available to discuss these matters with you.

DAVID A. VAUDT, CPA
Auditor of State

WARREN G. JENKINS, CPA
Chief Deputy Auditor of State

cc: Honorable Chester J. Culver, Governor
Charles J. Krogmeier, Director, Department of Management
Director, Legislative Services Agency

Tuition and Fees System General and Application Controls

A. Background

The tuition and fees system at the University of Northern Iowa (University) is a legacy system used to calculate and assess tuition and mandatory fees for enrolled students, to provide management with enrollment statistics and to generate student billing information for the accounts receivable system.

B. Scope and Methodology

In conjunction with our audit of the financial statements of the University, we reviewed selected aspects of the general and application controls in place over the tuition and fees system for the period May 24 through July 3, 2007. Specifically, we reviewed the general controls: security program planning and management, access controls, application software development and change controls, system software controls, segregation of duties and service continuity and the application controls: input, processing and output controls. We interviewed staff of the University and we reviewed University policies and procedures. To assess the level of compliance with identified controls, we performed selected tests.

We planned and performed our review to adequately assess those University operations within the scope of our review. We developed an understanding of the University's internal controls relevant to the operations included in the scope of our review. We believe our review provides a reasonable basis for our recommendations.

We used a risk-based approach when selecting activities to be reviewed. We focused our review efforts on those activities we identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, we used our finite review resources to identify where and how improvements can be made. Thus, we devoted little effort to reviewing operations that may be relatively efficient or effective. As a result, we prepare our review reports on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address activities that may be functioning properly.

C. Results of the Review

As a result or our review, we found certain controls can be strengthened to further ensure the reliability of financial information. Our recommendations, along with the University's responses, are detailed in the remainder of this report.

General Controls

(1) Password Controls – User ID's and passwords identify and authenticate users in controlling access to system resources. Passwords, however, are not conclusive identities of specific individuals since they may be guessed, copied, overheard or recorded and played back. Typical controls for protecting information resources include the use of strong passwords which are at least 8 characters in length, include a combination of alpha, numeric and special characters, are changed every 60 to 90 days, are not allowed to be reused and are locked out after a limited number of consecutive unsuccessful attempts. Passwords for the Time Share Option (TSO) and Consumer Information Control System (CICS) include several of these control features but other control features are not present. Additionally, group user ID's should not be allowed and payroll or personnel files should be compared to user ID's to remove terminated users in a timely manner.

Recommendation – The University should implement security features to strengthen password controls.

Response – In the short term, the University plans to modify, to the extent possible, the existing authentication system to implement stronger password controls. In the longer term (3-5 years), we plan to replace all the legacy student information systems currently residing on this outdated technology and migrate to a modern technology platform where we will be able to utilize the University's central authentication system which includes all the controls described above.

Conclusion – Response accepted.

(2) Security Profile Changes – Security profiles or authorized access rights help protect against tampering or unauthorized changes. Changes to security profiles by security managers granting administrative or system access rights are not automatically logged and periodically reviewed by management independent of the security function.

Recommendation – The University should enable or establish security features to ensure all security profile changes granting administrative or system rights are logged and are periodically reviewed by management independent of the security function.

Response – The University agrees that security profile changes should be logged and subsequently reviewed by management. Current procedures will be reviewed and adjusted accordingly.

Conclusion – Response accepted.

(3) Risk Assessments – A comprehensive high-level risk assessment is the starting point for developing or modifying the University's security policies and plan. Such risk assessments are important to help ensure all threats and vulnerabilities are identified, the greatest risks are considered and appropriate decisions are made regarding which risks to accept and which to mitigate through security controls.

Information Technology Services (ITS) personnel indicated a vulnerability assessment was conducted in 2005 on their network by an outside firm and a number of informal risk assessments have been performed. However, there is no evidence informal risk assessments have been conducted.

Recommendation – ITS should work with University administration to establish policies and procedures to conduct periodic formal risk assessments of critical financial applications.

Response – We agree that high level risk assessments are a necessary step in protecting critical financial applications and processes. While IT staff play an important role in identifying and mitigating some of the risk associated with financial processes, we believe that leadership for high-level assessment is better managed by data custodians or as part of the overall University risk management program. ITS will work with data custodians and risk management staff to initiate appropriate processes.

Conclusion – Response accepted.

(4) Comprehensive Background Checks – The University has a policy requiring comprehensive background checks for designated positions. Information Technology Services (ITS) has not designated positions requiring comprehensive background checks be performed before the employee is hired into a position enabling them to access, distribute or destroy confidential data. In addition, the University does not require documentation regarding reference checks be retained.

Recommendation – ITS should designate which positions are considered sensitive and require the performance of comprehensive background checks before hiring and documentation regarding the reference and background checks should be retained.

Response – ITS has provided the Provost's Office with a recommendation that criminal background checks be performed prior to hiring all permanent employees. Criminal background checks have been completed on all new hires since Fall 2007. The current draft of a new University Pre-Employment Background Check policy calls for a pre-employment criminal background check for the selected candidate.

Conclusion – Response accepted.

(5) System Access – Access to the Time Share Option (TSO) and Consumer Information Control System (CICS) is assigned according to the employee's job responsibilities and needs. Authorization is granted by the employee's department head/supervisor and by the application owner. The following instances were noted where procedures did not appear to effectively restrict access according to management's wishes:

a) Three user ID groups have been utilized which do not uniquely identify and authenticate users of TSO.

b) Access rights for 4 employees/students to TSO were not removed in a timely manner after they terminated employment.

c) Access rights for 17 employees/students to CICS in the Admissions Office were not removed in a timely manner after they terminated employment or transferred to another department.

d) Access rights for 3 employees/students to CICS in the Registrar's Office were not removed in a timely manner after they terminated employment or transferred to another department.

Recommendation – Procedures should be implemented to periodically review access rights to ensure access rights granted are in accordance with management's authorizations and remain appropriate for the current job responsibilities and needs of the employee.

Response – The University plans to modify current access procedures to automatically remove access rights upon termination of employment rather than depending upon departments to notify security administrators of such events.

Conclusion – Response accepted.

(6) System Software Modifications – Formal policies and procedures should exist for requesting and authorizing new or modified system software. At a minimum, policies should include the use of a change request system, acceptance testing, documentation of management review and approval, a chronological record of changes and a problem log for tracking and troubleshooting system software.

While a process has been implemented, including a change request form and management approval documentation, formal written policies and procedures for system software changes do not exist.

Additionally, changes are not reviewed and approved by someone other than the original installer.

Recommendation – The University should implement written policies and procedures for system software modifications and procedures requiring the review of system software changes by someone independent from the individual making the change.

Response – A written policy for system changes will be developed. System software change request procedures will be written. Change requests are now being sent to the system Programmer's supervisor for review and these documents are archived for future reference.

Conclusion – Response accepted.

(7) Manual Billing Adjustments – Student billings for tuition and fees can be adjusted manually by individuals within the Registrar's Office. In some cases, supporting documentation from the student is required, while in other cases a determination is made based on the reviewer/investigator's judgment. Although a written policy exists regarding a possible refund of tuition for students who drop classes, few written policies or procedures exist regarding the authorization and support of manual adjustments to billings.

Recommendation – Written policies and procedures should be established regarding the authorization and support of manual adjustments to billings. Changes to student billings for tuition and fees should be handled through the automated billing system when possible.

Response – Changes to student billings for tuition and fees are handled through the automated billing system when possible. Written policies and procedures will be established jointly by the Registrar's Office and the Office of Business Operations regarding the authorization and support of manual adjustments to billings when adjustments can not be made through the automated billing system.

Conclusion – Response accepted.

(8) Migration of Programs to Production – The establishment of controls over the modification of application programs helps to ensure only authorized programs and authorized modifications are implemented. This can be accomplished by instituting policies, procedures and techniques to ensure all programs and program modifications are properly authorized, tested and approved and access to programs is carefully controlled.

Access to the program is controlled, but programmers have access to other mainframe programs after they are submitted for review but before the program is placed into production.

Recommendation – The University should establish controls to ensure programmers do not have access to a program after submitting it for review and before promotion to production.

Response – The University plans to review existing procedures and make changes necessary to ensure all programs and program modifications are properly authorized, tested, and approved and access to programs is carefully controlled.

Conclusion – Response accepted.

(9) Contingency Plan – Losing the capacity to process, retrieve and protect information maintained electronically can significantly affect a University's ability to accomplish its mission. For this reason, the University should have procedures in place to protect information resources and minimize the risk of unplanned interruptions and a plan to recover critical operations should interruptions occur.

In 2000, the University developed/updated a contingency plan for Information Technology Services recovery in the event of a disaster. However, the University does not periodically test the contingency plan.

Recommendation – The University should update the contingency plan on a regular basis and periodically test the plan.

Response – The Student Information System contingency plan will be updated this year. Since this system is scheduled to be replaced in the next 3-5 years, we will schedule a review of this contingency plan at least one more time during the service life of the system.

Conclusion – Response accepted.

Application Controls

(1) Tuition and Fee Rates – Tuition and fee rates were approved by the Board of Regents at its December 11, 2006 meeting for the Summer 2007, Fall 2007 and Spring 2008 semesters. All tuition rates were properly assessed and posted to the billing system. However, in certain instances, several of the mandatory fee rates did not correspond with the rates approved by the Board of Regents. Certain health facility, health fees and building fees were not assessed in accordance with Board approved rates. The incorrect rates were provided by the Registrar's Office to programmers who coded those rates into the application.

Recommendation – Procedures should be established to verify mandatory fees are assessed at the rates approved by the Board of Regents.

Response – The Excel spreadsheet created for internal uses on January 5, 2007 correctly shows all tuition and fees as identified on page 10 of agenda item 7 of the December 11, 2006 Board of Regents Agenda. The PAR (programming authorization request submitted to ITS on 4-5-07 shows the correct amounts for tuition and fees as approved by the Board of Regents. In the narrative to tuition and fees on page 9 of the same document an error exists relative to the Health Facility Fee. The document cites that a flat fee is assessed to all students where in reality the full fee is assessed to those students taking 5 or more hours and a half time rate for those students taking 4 or fewer hours. Again, the grid showing tuition and fees on page 10 correctly reflects the half time rate amount. At our request the narrative on fees for fy09 was corrected to reflect the actual practice on assessment of the Health Facility Fee to students taking 4 or fewer hours.

In reviewing the Health Fee it should be noted that this is a single fee assessed beginning with 3 hours in the summer and at 5 hours in a semester. I believe the actual programming and assessment reflects this policy. The discrepancy in the building fee may be explained by understanding that the determination of half time in the summer is based on five credit hours while that determination is six hours in a semester.

Conclusion – Response accepted.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Darryl J. Brumm, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Billie Jo Heth, CPA, Senior Auditor
Shawn R. Elsbury, Staff Auditor