OFFICE OF AUDITOR OF STATE
STATE OF IOWA

State Capitol Building
Des Moines, Iowa 50319-0004

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

David A. Vaudt, CPA
Auditor of State

NEWS RELEASE

Contact: Andy Nielsen
515/281-5834

FOR RELEASE September 13, 2010

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 Accounts Payable/Purchasing System for the period of June 10, 2009 through August 20, 2009.

Vaudt recommended the University of Northern Iowa establish procedures to increase security, strengthen accountability and update its business continuity/disaster recovery plans. The University has responded positively to the recommendations.

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/1061-8030-BT01.pdf

# # #

REPORT OF RECOMMENDATIONS TO THE UNIVERSITY OF NORTHERN IOWA ON A REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE UNIVERSITY'S ACCOUNTS PAYABLE/ PURCHASING SYSTEM

JUNE 10, 2009 THROUGH AUGUST 20, 2009

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

August 27, 2010

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

In conjunction with our audits of the financial statements of the University of Northern Iowa for the years ended June 30, 2010 and 2009, we conducted an information technology review of selected general and application controls for the period June 10, 2009 through August 20, 2009. Our review focused on the general and application controls of the University's Accounts Payable/Purchasing System as they relate to our audits 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 Accounts Payable/Purchasing system. These recommendations have been discussed with University personnel and their responses to these recommendations are included in this report. While we have expressed our conclusions on the University's responses, we did not audit the University's responses and, accordingly, we express no opinion on them.

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 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 of the University's Accounts Payable/Purchasing System are listed on page 9 and they are available to discuss these matters with you.

David A. Vaudt | Warren Jenkins

DAVID A. VAUDT, CPA
Auditor of State

WARREN G. JENKINS, CPA
Chief Deputy Auditor of State

cc: Honorable Chester J. Culver, Governor
Richard C. Oshlo, Jr., Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

Accounts Payable/Purchasing System General and Application Controls

A. Background

The Accounts Payable/Purchasing System at the University of Northern Iowa (University) includes the purchase order/requisition system which allows requisitions to be entered online using the Oracle purchasing system. The requisition must bear the electronic approval of the department head or authorized official and is routed to the Purchasing Department for a purchase order or quote. Responses to quotes are documented and reviewed by the buyer and copies of the bid responses and recommended vendor are sent to the requesting department for review. A purchase order is prepared in the Purchasing Department, signed by the purchasing manager and matched to an approved requisition and then emailed or faxed to the vendor. To make a payment on a purchase order, an invoice must be received from the vendor and entered into the system by Accounts Payable staff. The requesting department must enter the receipt of the goods or services in the Oracle purchasing system. Once the department enters the receipt of the goods or services, a match is created with the invoice and the vendor is paid.

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 University's accounts payable/purchasing system for the period June 10, 2009 through August 20, 2009. Specifically, we reviewed the general controls: security program planning and management, access controls, configuration management, 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 use our finite review resources to identify where and how improvements can be made. Thus, we devote 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 of 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) Risk Assessments – Periodic risk assessments should be conducted to help ensure all threats and vulnerabilities are identified and considered, the greatest risks are identified and appropriate decisions are made regarding which to accept and which to mitigate through security controls. The University does not have a formal risk assessment policy. Vulnerability scans are performed periodically, but a formal risk assessment has not been conducted and documented.

Recommendation – The University should develop formal procedures to periodically conduct and document risk assessments at both University-wide and departmental levels.

Response - The University acknowledges high level risk assessments are a necessary step in protecting critical university data and processes. Information Technology Services (ITS) will work with UNI Administration to develop a risk assessment program and, in particular, risk associated with the collection, storage, and transmission of information as defined within ISO 27001:2005.

Conclusion – Response accepted.

(2) 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. 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. The MEMFIS – Accounts Payable system includes a number of these controls, but they could be strengthened.

Recommendation – The University should take steps to strengthen password controls.

Response – Information Technology Services (ITS) is currently evaluating several options for integrating the Oracle E-Business Applications (MEMFIS) with the University's central authentication system called CatID. Several administrative applications including student information systems, email, eLearning, imaging and others already use the CatID. More restrictive standards have been established for the CatID authentication system. The CatID system requires passwords which are at least 8 characters in length, requires a combination of alpha, numeric and special characters, and must be changed every 90 days. Passwords cannot be reused and includes a lockout feature after 10 consecutive unsuccessful attempts. ITS plans to transition the MEMFIS applications to the CatID system during the next 6-12 months.

Conclusion – Response accepted.

(3) Confidentiality Agreements – Confidentiality agreements serve as a reminder to staff and contractors of their responsibilities regarding the protection and safeguarding of confidential resources and information maintained by the University. All ITS employees and contractors with access to confidential information are required to sign a confidentiality agreement. One ITS employee tested did not have a signed confidentiality agreement on file.

Recommendation – The University should ensure all employees and contractors with access to confidential information sign confidentiality agreements and these agreements should be kept on file.

Response – Information Technology Services (ITS) confidentiality agreements are signed as a condition of employment. For existing staff refusing to sign this agreement, we will review the requirements of this agreement as part of the annual performance review. ITS will work with Human Resource Services and administrative and academic department heads to develop a university-wide confidentiality policy for both current and future employees.

Conclusion – Response accepted.

(4) Computer Room Access – Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Access should be limited to personnel with a legitimate need for access to perform their job duties.

We identified two individuals who had access to the computer room who were no longer employed at the University.

Recommendation – The University should establish procedures to ensure access is removed immediately for employees who leave University employment or no longer need access to perform their duties.

Response – Since June of 2009, Information Technology Services (ITS) has reviewed the list of technology staff members with access to ITS managed computer rooms in Gilchrist Hall and the Curris Business Building on a quarterly basis. Quarterly reviews will be made by ITS, Public Safety and Physical Plant to verify timely removal of terminated employees. To further improve computer room access monitoring, video cameras and visitor log books will be added at both locations.

Conclusion – Response accepted.

(5) Program Test Standards – A disciplined process for testing and approving new and modified programs prior to their implementation is essential to make sure programs operate as intended and unauthorized changes are not introduced. Once a change has been authorized, it should be written into the program code and tested in a disciplined manner. Because testing is an interactive process generally performed at several levels, it is important the University adhere to a formal set of procedures or standards for prioritizing, scheduling, testing and approving changes.

System and program testing standards have not been formalized or approved for all levels of testing defining responsibilities for each party.

Recommendation – The University should formally adopt testing standards and identify at what levels testing is required.

Response – Separate development, test, and production systems are currently maintained for the MEMFIS applications. Testing is completed by both development staff and by functional offices prior to being moved to production. Information Technology Services (ITS) will work with administrative offices to review current procedures and to formalize standards and procedures for testing new and/or modified software.

Included will be testing requirements (scope), testing approach, estimates, testing phases, testing schedule, completion criteria, test environment and team roles and responsibilities.

Conclusion – Response accepted.

(6) Vulnerability Scans and Penetration Testing – Internet–borne attacks targeting security vulnerabilities occur on a daily basis and can threaten assets and mission critical systems. A proven way to reduce risks from attack is to proactively test systems and implement appropriate counter measures. Vulnerability assessments are a valuable tool in this process and help in gauging the effectiveness of security measures.

A policy has not been established to address vulnerability scans and penetration testing.

Recommendation – The University should establish a policy to address vulnerability scans and penetration testing.

Response – The ITS Security Office currently performs voluntary vulnerability scans on campus resources for all campus units on a quarterly basis. Results from these scans are shared with the responsible system administrators and retained by ITS Security Office. ITS will develop a policy requiring vulnerability scans and penetration testing for systems identified as storing critical assets and resources.

Conclusion – Response accepted.

(7) Review of Accounts Payable Responsibilities – Each department of the University is responsible for granting, deleting and checking the appropriateness of employee access to departmental resources. Four individuals were noted who still had access to the Accounts Payable system but had previously transferred to other areas of the University or retired.

Recommendation – The Office of Business Operations should periodically review users' access rights to ensure access rights granted remain appropriate for the current job responsibilities and needs of the employee.

Response – The University acknowledges the need to periodically review employee access rights and ensure they are appropriate for the employee's job responsibilities. The Office of Business Operations (OBO) has instituted a process of terminating access rights immediately following the end of an employee's employment in OBO. A secondary review is performed annually to ensure employee access rights are still appropriate for all OBO employees. The University also has an automated procedure to terminate all non self-service access as of the date the employee is terminated in the human resource management system.

Conclusion – Response accepted.

(8) Business Continuity/Disaster Recovery plans – Disaster recovery plans are designed to help ensure the University remains functional in the unlikely event of a loss of facilities or personnel. These plans should be updated regularly, periodically tested, distributed to key individuals and maintained in written form at an off-site location. In addition, the plan has not been tested with a full walk through of a disaster situation.

Recommendation – The University should update its business continuity/disaster recovery plans regularly and distribute it to all individuals who are expected to play a key role if the plan is put into action. Also, a copy of the plan should be stored at an off-site location and the plan should be tested periodically.

Response – The disaster recovery plan for the University's financial information systems (Oracle E-Business) will be updated during the upcoming year. The disaster recovery plan for the legacy student information systems (mainframe) was updated during the past year. All systems currently residing on the mainframe will be replaced by the new student information system (PeopleSoft Campus Solutions) slated for implementation by the end of June 2011. A new disaster recovery plan will be developed to support this new software/hardware environment.

Copies of the disaster recovery plans will be stored by each ITS Director at their residence.

After completing the update to the Oracle E-Business disaster plan ITS management will call for an unannounced test of the plan. The plan will be tested using the Gilchrist Hall computer room and equipment currently housed at that location including the storage area network. The Gilchrist Hall computer room is used primarily for test systems and serves as a disaster recovery location for many of the production systems located in the Curris Business Building including the Oracle E-Business systems. Functional area personnel will be utilized to validate the results of the testing.

Conclusion – Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the University's Accounts Payable/Purchasing System.

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, Senior Auditor II
Aaron P. Wagner, CPA, Staff Auditor
Kurt D. Goldsmith, Assistant Auditor