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

Contact: Andy Nielsen
515/281-5834

FOR RELEASE October 6, 2004

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 Modern Executive Management Financial Information System (MEMFIS) for the period June 7, 2004 through July 29, 2004.

Vaudt recommended the University develop and implement a University-wide security plan, establish formal system and program test standards, develop system software change review procedures, ensure segregation of duties is maintained and review procedures for daily backup tape storage.

A copy of the report is available for review at the University of Northern Iowa or the Office of Auditor of State.

###

REPORT OF RECOMMENDATIONS TO THE UNIVERSITY OF NORTHERN IOWA ON A REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE MODERN EXECUTIVE MANAGEMENT FINANCIAL INFORMATION SYSTEM

JUNE 7, 2004 to JULY 29, 2004

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

July 29, 2004

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, 2004, we have conducted an information technology review of selected general and application controls for the period June 7, 2004 through July 29, 2004. Our review focused on the general and application controls for the Modern Executive Management Financial Information System (MEMFIS) 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 MEMFIS 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 MEMFIS. 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 9 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 Thomas J. Vilsack, Governor
Cynthia P. Eisenhauer, Director, Department of Management
Dennis C. Prouty, Director, Legislative Services Agency

Modern Executive Management Financial Information System (MEMFIS) General and Application Controls

A. Background

The MEMFIS Project at the University of Northern Iowa (University) is a campus-wide initiative with the primary objective of replacing the core systems of human resources, payroll, general ledger, purchasing, accounts payable, grants and contracts, projects and budgeting. As of the date of our review, the general ledger, purchasing, cash management and accounts payable applications were in place.

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 MEMFIS for the period June 7 through July 29, 2004. Specifically, we reviewed the following general controls: University-wide security program planning and management, access controls, application software development and change controls, system software controls, segregation of duties and service continuity and the following application controls: input, processing and output controls for the general ledger and accounts payable. 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 control 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) 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.

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

Response – Information Technology Services will ask the University Cabinet to fund a new position to develop University-wide risk assessment procedures. Given the current budget situation we are not optimistic funding will be provided in the near future.

Conclusion – Response acknowledged. Until a formal University-wide risk assessment is funded, informal risk assessments currently performed on system developments and modifications should be formalized, documented and expanded to the extent possible with existing staff.

(2) Security Plan – A written security plan should clearly describe the University's security program and the supporting policies and procedures and it should be available to all affected employees. Best practices call for the plan and related policies to cover all major systems and facilities and outline the duties of those who are responsible for overseeing security, as well as those who manage, use or rely on the University's computer resources.

Our review indicated policies and procedures are in draft form awaiting review and approval and a comprehensive written security plan has not yet been approved.

Recommendation – The University should complete the development, approval and implementation of a written security program covering all major systems and facilities and outlining duties of those responsible for overseeing security, as well as those who manage, use or rely on the University's computer resources. The plan should be distributed to all affected employees.

Response – Information Technology Services has already identified as its top priority the need for a campus wide security administrator position. This individual would develop a written security program and oversee the implementation and monitoring of the established policies and procedures. Funding for this position has not yet been provided and given the current budget situation we are not optimistic that it will be provided in the near future.

Conclusion – Response acknowledged. Until a campus-wide security administrator is appointed and a University-wide security program is implemented, the University should complete the draft Network Citizenship Guideline and Procedures and Campus Network Policy which, along with existing Use of Computer Resources and World Wide Web policies, address a number of the security issues.

(3) Comprehensive Background Checks – The University does not require comprehensive background checks be performed before an 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 – The University should establish policies and procedures requiring comprehensive background checks be performed before hiring individuals in sensitive positions and documentation regarding the reference and background checks should be retained.

Response – The University does have a background check policy (http://www.uni.ed\pres\policies\430shtml). Information Technology Services plans to designate those IT positions requiring checks in the upcoming fiscal year.

Conclusion – Response accepted.

(4) Confidentiality Agreements – The University does not have a policy requiring employees and contractors to sign confidentiality and security agreements when using confidential information.

Recommendation – The University should develop formal written policies covering confidentiality and security agreements to be signed by employees and contractors who use confidential information.

Response – Information Technology Services staff will contact our sister institutions to get examples of policies and confidentiality agreements used at those universities. We will then develop an agreement that we will follow and will encourage other UNI departments handling confidential information to use it as well.

Conclusion – Response accepted.

(5) 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. The following were noted:

(a) Monitoring of computer room after hours access was limited.

(b) Visitors are not required to sign-in and out on when entering or leaving the ITS Network Services area.

Recommendation – The University should consider:

(a) Strengthening the monitoring of after hours access of the computer room.

(b) Requiring visitors to sign in and out when entering the ITS Network Services area.

Response –

(a) Improvements will be installed when funding is made available. It has been included in our building repairs request for the past several years.

(b) Visitors are not allowed into locked computer operation rooms. Visitors wishing to meet with staff in these areas are met and escorted by appropriate staff. We see no benefit in having staff sign in and out when entering.

Conclusion – Response acknowledged. A sign in log would document who visited the computer room when that information is necessary.

(6) Password Control – Logical access controls involve the use of user ID's and passwords to control access to system resources. The number of times access can be attempted for the MEMFIS applications before an account is locked out is not restricted.

Recommendation – The University should implement security features to limit the number of times access can be attempted on the MEMFIS applications.

Response – We will implement this by the end of the year.

Conclusion – Response accepted.

(7) Written Policies and Procedures – Application software development and change control procedures include development of a detailed test plan for each modification defining levels and types of tests to be performed and responsibilities for each person involved in testing and approving software.

System and program testing standards have been established for larger changes, but not for all levels of testing. Responsibilities of each party have not been defined. Also, test plans have not been documented and approved.

Recommendation – The University should establish system and program testing standards for all levels of testing and define responsibilities for each party.

Response – Detailed test plans have already been developed for the Oracle Financial Information systems implemented in phase I of the MEMFIS project. Test plans are currently being developed for the modules that will be implemented as part of Phase II. These test plans will be executed each time the Oracle applications are upgraded. We do not currently have documented test plans and procedures for making custom changes to the Oracle applications. Custom changes to the phase I Oracle applications are currently frozen but once we resume making changes we plan to implement procedures that require documented test plans along with the already established sign-off procedures.

Conclusion – Response accepted.

(8) System Software Changes – Best practices call for system software and emergency changes to be reviewed by someone with supervisory authorization other than the original installer.

Changes are not reviewed and approved by someone other than the original installer. Emergency changes are not reviewed by an independent IS supervisor.

Recommendation – The University should establish procedures requiring review of system software changes by someone independent from the individual making the change.

Response – All production software changes are approved by Kevan Forest. However, we currently do not "audit" that what was said would be done, against what was actually done. We will ask Melanie Abbas to audit at least one of every 10 system software changes.

Conclusion – Response accepted.

(9) Workflow Duties – The University MEMFIS system grants access to users through use of responsibilities when access is set-up.

Individuals tested were identified as having access to responsibilities not necessary for their job duties, as follows:

- Eight individuals were identified as having access to the UNI General Ledger Supervisor responsibility that did not appear to need that level of access.

- One individual was identified as having access to the UNI Payables Specialist responsibility that did not appear to need that level of access.

Certain responsibilities allow a user to perform multiple financial functions incompatible for proper segregation of duties, as follows:

- UNI General Ledger Super User and UNI General Ledger Supervisor gives the user the ability to initiate or enter and post journal entries.

- UNI Payables Manager and UNI Cashier both give the user the ability to enter an invoice, apply approval and make payment or cut the check.

Recommendation – The University should review the list of those with access to the back office responsibilities and ensure access is granted only for necessary job duties and at the appropriate level of access.

The University should develop a new workflow control in MEMFIS to prevent a user from posting a journal entry they entered initially and prevent a user from making payment or cutting a check for an invoice they approved.

Response – Lists of users with the various back office responsibilities have been provided to the system owners. They are reviewing the lists and will provide us with signed authorization change sheets indicating any changes they feel are warranted.

Conclusion – Response acknowledged. If software enhancements are not available to prevent individuals from performing incompatible functions, segregation of duties should be strictly enforced as roles and responsibilities are assigned in MEMFIS. The activity of super users should be logged and reviewed by management.

(10) Off-site Daily Back Up Tape Storage – Routinely copying data and software files and securely storing these files at a remote location are usually the most cost effective actions the University can take to mitigate service interruptions. The University maintains backup tapes at a separate off-site location for weekly, monthly and yearly data. A review of procedures revealed daily back up tapes are not kept at an off-site storage location.

Recommendation – The University should review existing procedures to ensure daily back up tapes are stored at an off-site storage location.

Response – This enhancement is in progress and should be complete by the end of this calendar year.

Conclusion – Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the University's MEMFIS system.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Brian R. Brustkern, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Darryl J. Brumm, CPA, Senior Auditor II
Heather B. Allen, Staff Auditor