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 December 31, 2003

Auditor of State David A. Vaudt today released a report on the 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 2 through July 17, 2003.

Vaudt recommended that the University develop and implement procedures to improve physical security controls, logical access controls, system software controls, disaster recovery plans, daily backup procedures, and system and program test standards.

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

# # #

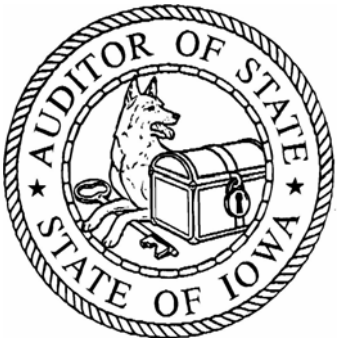
REPORT OF RECOMMENDATIONS TO THE UNIVERSITY OF NORTHERN IOWA ON THE REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE MODERN EXECUTIVE MANAGEMENT FINANCIAL INFORMATION

JUNE 2 TO JULY 17, 2003

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 17, 2003

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, 2003, we have conducted an information technology review of selected general and application controls for the period June 2 through July 17, 2003. 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 those 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 that 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 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 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

cc: Honorable Thomas J Vilsack, Governor
Cynthia P. Eisenhauer, Director, Department of Management
Dennis C. Prouty, 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 2 through July 17, 2003. Specifically we reviewed the general controls: access controls, application software development and change controls, system software and service continuity; and the application control: input controls for the general ledger and accounts payable. We interviewed staff from 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 that are within our review scope. We developed an understanding of the University's internal control that is relevant to the operations included in our review scope. We believe our review provides a reasonable basis for our recommendations.

We use a risk-based approach when selecting activities to be reviewed. We therefore focus our review efforts on those activities we have 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 that certain controls can be strengthened to further ensure the reliability of financial information. Our recommendations, along with the University's responses, are listed in the remainder of this report.

General Controls:

(1) 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.

(a) A number of physical plant employees have access to the ITS Computer Room in the Curris Business Building (CBB), but they did not appear to need access to perform their job duties.

(b) The computer room within the ITS Network Services area has three access doors, two of which are left unlocked during portions of the day. There is also no security system in place for the computer room to monitor after hours access.

(c) There is no sign in log that visitors are required to sign in and out on when entering or leaving the ITS Network Services in the Curris Business Building. Also, a receptionist is not currently stationed at the main entrance.

Recommendation – The University should consider the following:

(a) Re-keying the computer room using a more secure key to limit the number of individuals with access to that area.

(b) Keeping the doors to the inner computer room locked at all times along with installing a security system to monitor after hours access.

(c) Requiring visitors to sign in and out when entering the ITS Network Services (NS) area along with stationing a receptionist at the entrance during business hours.

Response –

(a) Keyed access to ITS computer room is restricted to UNI employees that have a need to work in this area. This list would include: All ITS Network Services staff and other ITS System Administrators that have systems residing in these rooms.

ITS relies upon the UNI Physical Plant and Public Safety departments for physical maintenance and security of this facility. This support is governed by operating procedures of these departments and includes the following types of individuals. Physical Plant trade staff (electricians, cooling/heating staff and carpenters) have access to deal with facility failures. Physical Plant Custodial staff serving CBB and their supervisors have access to this facility. UNI Public Safety officers have access to this facility.

ITS will work with Physical Plant administration, to see if access to this area can be managed differently than other UNI spaces. ITS direct support of electrical, environmental, carpentry, custodial services would be cost prohibitive.

(b) The inner computer rooms have four access doors.

#1 Entry to the room from the hallway; Currently it is locked with storage area lockset.

#2 Entry to the room from the hallway; Currently a dutch-door locked with storage area lockset.

#3 Entry to the room from another room; Currently it is unlocked.

#4 Entry to the room from another room; Currently it is unlocked.

ITS proposes the following measures to improve security surrounding physical access to the inner computer rooms:

#1 will remain as is. Permanently locked with storage area lockset.

#2 will have upper door closed and left locked with storage area lockset.

#3 will have keypad and electronic strike.

#4 will have keypad and electronic strike.

As funds become available ITS will pursue installation of room security system for after hours access to cover rooms in ITS area.

(c) Receptionist has been added to CBB. This will improve the direction of visitors seeking NS staff and eliminate the need to send non-ITS staff through the inner computer rooms. Coupling the reception function with locking of the inner computer room doors will dramatically reduce the non-ITS staff entering the computer rooms. ITS sees little value in requiring a sign-in when vast majority of traffic in this area will be restricted to the CBB office area.

Conclusion – Response accepted.

(2) Password Control – Logical access controls involve the use of user ID's and passwords to control access to system resources. The following items related to passwords for the University's MEMFIS System were noted:

(a) Passwords for access to UNIX on the servers are not required to be changed at regular intervals.

(b) A large number of inactive user ID's exist.

(c) There is no limit to the number of times access can be attempted for the MEMFIS applications.

Recommendation – The University should implement security features that include requiring password changes at regular intervals for the UNIX servers and limiting the number of times access can be attempted on the MEMFIS applications. The University should also consider developing procedures to periodically review the list of authorized users for propriety.

Response –

(a) Passwords are currently required to be changed every six months, but this still does not meet auditor requirements. As a result we will be expiring passwords every 3 months.

(b) This is currently true for the MEMFIS applications themselves. We currently have a process in place to ensure old inactive student accounts are removed from the system, but not for Faculty and Staff. We will extend that process so that at least once a year we review all accounts and ensure they are still valid and being used.

(c) The Oracle applications software (MEMFIS), which is a vended software package, does not currently provide this functionality. We will look at filing an enhancement request with Oracle, to suggest that they add this.

Conclusion – Response accepted.

(3) System Software Changes – System software changes and emergency changes should be reviewed by someone with supervisory authorization other than the original installer. The changes should be implemented by someone other than the original programmer.

Changes are not reviewed and approved by someone other than the original installer. A separate review of emergency changes is not done by an independent IS supervisor.

Recommendation – The University should establish procedures that require review of system software changes by someone other than the individual making the change.

Response – This refers to our UNIX system environment in which our regularly scheduled maintenance is documented and communicated via e-mail, but not officially signed off. The manager of the technical team will respond to these messages via e-mail with a yes or no authorization and file these for future auditor review.

Conclusion – Response accepted.

(4) Disaster Recovery Plan – Losing the capability to process, retrieve and protect information maintained electronically can significantly affect an entity's ability to accomplish its mission. For this reason, an entity should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. The University has developed a disaster recovery plan for the MEMFIS system in the event of a disaster that is currently in draft form. This plan has not been formally adopted, a copy is not currently kept off-site, and there is no provision for testing the plan.

Recommendation – The University should adopt and distribute a disaster recovery plan, maintain a copy off-site, and develop procedures for periodically testing the plan.

Response – We have developed a recovery plan for the University Financials (MEMFIS) system. We are currently obtaining management approval of the plan. Once approved, copies will be placed in both the Gilchrist Hall Vault, as well as in the US Bank vault, located in Cedar Falls. Our goal for completing this is October 2003.

Conclusion – Response accepted.

(5) Off-site Daily Back Up Tape Storage – Routinely copying data files and software and securely storing these files at a remote location are usually the most cost effective actions that an entity 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 that daily back up tapes are not kept at an off-site storage location.

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

Response – We are currently working with various parties on campus to transport our tapes on a daily basis from the Curris Business Building where the computer room is, to Gilchrist Hall. The controller's office in Gilchrist Hall has indicated they will allow us to store our daily tapes in their vault. We expect this to be implemented by the end of 2003.

We are already sending our weekly tapes off site to a bank here in Cedar Falls. This effort will continue even after we start sending daily tapes to Gilchrist.

Conclusion – Response accepted.

(6) Written Policies and Procedures – Application Software Development and Change Control procedures should include development of a detailed test plan for each modification that defines the levels and types of tests to be performed and defining 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 for 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 that define responsibilities for each party.

Response – We currently have a good pool of test cases which are used for major installs and projects. We will now require that test cases be developed and executed for all modifications regardless of size.

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:

Steven O. Fuqua, CPA, Senior Auditor
Cory A. Warmuth, CPA, Staff Auditor
Donald N. Miksch, Assistant Auditor
Ryan J. Johnson, Assistant Auditor