

MEMORANDUM

To: Banking Committee
From: Board Office
Subject: State Audit Reports
Date: March 1, 2004

Recommended Action:

Receive the following Auditor of State reports on the review of selected general and application controls over the following:

UNIVERSITY OF IOWA

- Purchasing and Accounts Payable System

IOWA STATE UNIVERSITY

- Tuition System

UNIVERSITY OF NORTHERN IOWA

- Modern Executive Management Financial Information System
-

Executive Summary:

State audit reports are presented to the Banking Committee as required by Board policy. State Auditor David Vaudt will be available for any questions.

The State Auditor reviewed and evaluated the general and application controls of the University of Iowa's Purchasing and Accounts Payable System, Iowa State University's Tuition System, and the University of Northern Iowa's Modern Executive Management Financial Information System to determine whether controls were sufficient to provide reasonable, but not absolute, assurances that control objectives were achieved.

The auditor's opinion concluded that general controls for all three systems were sufficient, except for the identified findings. The universities are taking corrective action and the auditor's conclusions for all responses have been accepted or acknowledged.

Background:

In accordance with Regent Policy Manual §1.05, audit reports from the State Auditor are presented to the Banking Committee. Studies of university departments were initiated by the State Auditor during 2003 and are expected to continue as part of their annual review process. The reviews are conducted to study and evaluate departmental controls and/or to determine departmental compliance with university guidelines; the reports are not intended to constitute audits of the financial statements.

These audits are designed to determine whether controls were sufficient to provide reasonable, but not absolute, assurances that control objectives were achieved.

Corresponding tables highlight auditor recommendations, management responses, auditor responses, and whether corrective actions have been taken. Controls in the following key areas were studied:

General Controls:

- Access Controls
- Application Software Development and Change Controls
- Security Program
- Segregation of Duties and Service Continuity
- System Software and Service Continuity Controls

Application Controls:

- Input, Processing, and Output Controls

**The University of Iowa
Selected General and Application Controls over the
Purchasing/Accounts Payable System**

State Audit Report Issued: August 8, 2003

Recommendations/
Responses

Auditor's Recommendation	Management's Response
GENERAL CONTROLS	
1. <u>Activity Logs</u> . Establish procedures to record and monitor activity logs for unauthorized or unusual activity.	Management will upgrade to a newer version that does have this capability.
2. <u>Logical Access Controls</u> . Activate available features in software to enforce regular use of and frequent changing of passwords.	Management will deploy lockout features and other security protections as they become available in future software updates.
APPLICATION CONTROLS	
No findings reported.	N/A

**Iowa State University
Selected General and Application Controls over the Tuition System**

State Audit Report Issued: July 10, 2003

Auditor's Recommendation	Management's Response
GENERAL CONTROLS	
1. <u>Risk Assessments</u> . Establish procedures to conduct formal risk assessments.	Management will formalize processes already being practiced, develop a schedule for risk assessment, and document the results of the assessment.
2. <u>Security Plan</u> . Develop and approve a written security plan.	Management is developing a campus-wide security policy.
3. <u>Incident Response Capability</u> . Develop and implement an incident response capability.	Management will identify the need for a document to address responsibilities and procedures for identifying and reporting security breaches as part of the campus-wide security policy.
4. <u>Automatic Logoff</u> . Develop automatic logoff for system users after preset period of inactivity.	Management will implement automatic log off after four hours of inactivity.
5. <u>System Access for Terminated or Transferred Employees</u> . Develop and implement procedures to notify IT security when employees terminate employment or transfer.	Management will continue to develop procedures with the goal for completion to improve network and system access controls by the end of FY 2004.
6. <u>Promotion of Programs to Production</u> . Implement procedures to segregate duties between programmer, manager sign-off, and promotion to production.	Management has implemented significant source controls over the past several years and will continue to look to ways to improve and strengthen the process.
APPLICATION CONTROLS	
No findings reported.	N/A

University of Northern
Selected General and Application Controls over the Modern
Executive Management Financial Information System

State Audit Report Issued: July 17, 2003

Recommendations/
Responses

Auditor's Recommendation	Management's Response
GENERAL CONTROLS	
<p>1. <u>Computer Room Access.</u></p> <p>a. Re-key computer room using a more secure key to limit access to that area.</p> <p>b. Keep doors to inner computer room locked at all times and install a security system to monitor after hours access.</p> <p>c. Require visitors to sign in and out and station a receptionist at the entrance during business hours.</p>	<p>Management will work with physical plant administration to see if access to this area can be managed differently than other UNI spaces.</p> <p>Entry #1 will be permanently locked. Entry #2 will have upper door closed and left locked. Entries #3 and #4 will have keypad and electronic strike. Installation of a security system will be considered as funds become available.</p> <p>A receptionist has been added.</p>
<p>2. <u>Password Control.</u></p> <p>a. Require passwords for access to UNIX on the servers to be changed at regular intervals.</p> <p>b. Eliminate the large number of existing inactive user ID's.</p> <p>c. Limit access attempts for the MEMFIS applications.</p>	<p>Management will have passwords expire every three months.</p> <p>Management will implement annual review of all student, faculty, and staff accounts to ensure removal of inactive accounts.</p> <p>Management will file an enhancement request with Oracle for this addition.</p>
<p>3. <u>System Software Changes.</u> Establish procedures to require review of system software changes by someone other than the original programmer.</p>	<p>Management of the technical team will respond to e-mail documentation with a yes or no authorization by e-mail and file these for future auditor review.</p>
<p>4. <u>Disaster Recovery Plan.</u> Adopt and distribute a disaster recovery plan, maintain a copy off-site, and develop procedures for periodically testing the plan.</p>	<p>Management is currently reviewing a recovery plan for the University Financials (MEMFIS) system and will place copies in off-site locations.</p>

**University of Northern Iowa
Selected General and Application Controls over the Modern
Executive Management Financial Information System**

(continued)

Auditor's Recommendation	Management's Response
5. <u>Off-site Daily Back up Tape Storage.</u> Ensure that daily back up tapes are stored at an off-site storage location.	Management is working with various parties on campus to transport tapes on a daily basis from Curris Business Building to the vault in Gilchrist Hall. Weekly tapes are sent off-site to a bank in Cedar Falls.
6. <u>Written Policies and Procedures.</u> Establish system and program testing standards for all levels of testing that define responsibilities for each party.	Management currently has a good pool of test cases to use for major installations and projects and will expand them to include all modifications, regardless of size.
APPLICATION CONTROLS	
No findings reported.	N/A