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
FOR RELEASE December 29, 2003 515/281-5515

Auditor of State David A. Vaudt today released a report on the review of selected general and application controls over the Iowa State University of Science and Technology (Iowa State University) tuition system for the period of April 23 through May 23, 2003.

Vaudt recommended Iowa State University develop and implement procedures to improve information system controls related to security, system access and the migration of programs to production.

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

###

REPORT OF RECOMMENDATIONS TO
IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY
ON THE REVIEW OF SELECTED GENERAL AND
APPLICATION CONTROLS OVER
THE TUITION SYSTEM

APRIL 23 TO MAY 23, 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 10, 2003

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

In conjunction with our audit of the financial statements of Iowa State University of Science and Technology (Iowa State University) for the year ended June 30, 2003, we have conducted an information technology review of selected general and application controls for the period April 23 through May 23, 2003. Our review focused on the general and application controls of the tuition system 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 the tuition 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 Iowa State University, citizens of the State of Iowa, and other parties to whom Iowa State University 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 tuition system are listed on page 9, and they are available to discuss these matters with you.

David A. Vaudt

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

Tuition System General and Application Controls

A. Background

The tuition system at Iowa State University (University) is used to calculate, assess and record tuition charges for all students.

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 system for the period April 23 through May 23, 2003. Specifically we reviewed the general controls: security program, 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 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) Risk Assessments – Periodic risk assessments should be conducted to help ensure that all threats and vulnerabilities are identified, that the greatest risks are considered, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls.

University personnel indicated that no formal risk assessments have been conducted as of May 23, 2003.

Recommendation – The University should establish procedures to conduct formal risk assessments.

Response – Risk assessments are ongoing tasks that already take place in most units, especially those involved with financial transactions. Since the level of risks vary greatly, and the safeguards that the university implements to mitigate those risks to an acceptable level are related to the system or process, the risk assessment is best handled by the unit that is responsible for the system or process. The finding of this audit reveals a need for formalizing many of the processes that are already being practiced. Formalizing these processes is interpreted to mean developing a schedule to do the risk assessment and documenting the results of the risk assessment.

An Information Security Task Force (ISTF) was appointed by the President in March 2003 with the charge to evaluate current policies relating to information security and make recommendations for changes or additions. The overall security policy describes roles and responsibilities and it assigns the responsibility for completing a risk assessment to the unit that is the custodian for a system. The custodian will use the risk assessment to develop and implement appropriate security practices. The risk assessment should include a recommendation for the frequency of reviewing the risk and the security practices. The custodian has the responsibility to document the risk assessment along with appropriate security practices so they are available for future auditor review.

The focus of this audit was tuition assessment, which falls under the responsibility of the Registrar's office. The Registrar's office should set the schedule of the next risk assessment. Administrative Technology Services will support the Registrar's office as they do their risk assessment.

Conclusion – Response accepted.

2) Security Plan – A written security plan should clearly describe the University's security program and the policies and procedures that support it. The plan and related policies should 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. The security plan should be available to all affected employees.

Our review indicated policies and procedures are not always in writing and a comprehensive written security plan has not been approved.

Recommendation – The University should complete the development and approval of a written security program. The plan should also be distributed to all affected employees.

Response – There are many policies in place that address information security. There are also regulatory requirements for security programs in place (e.g. FERPA, HIPAA, GLB). The audit recommends that a campus-wide written security policy be drafted.

The ISTF is in the process of drafting a campus-wide security policy. The deliverables of the task force will include an overall policy plus a document of standards, guidelines, and best practices. The overall policy charges the custodians of the strategic application with the responsibility for risk assessment and implementing security practices. The ISTF has started an awareness campaign to various groups on campus. It is also developing a web site to provide information about security and information to help in doing risk assessments.

Conclusion – Response accepted.

3) Incident Response Capability – Security incidents, whether caused by viruses, hackers, or software bugs, are becoming more common. They also cause greater concern because systems are increasingly interconnected and security incidents can place many valuable resources at risk of corruption or disclosure. An incident response capability helps to contain and repair damage caused by an incident as well as to prevent future damage. Characteristics of a good incident handling capability are:

   - The required use of anti-virus software;
   - An understanding of the constituency being served, including computer users and program managers;
   - An educated constituency that trusts the incident handling team;
   - A means of prompt centralized reporting;
   - A response team with necessary knowledge, skills, and abilities; and
   - Links to other groups-such as law enforcement agencies, response teams, or security groups external to the organization

   No formal incident response capabilities or procedures have been established.

   Recommendation – The University should develop and implement an incident response capability.

   Response – The threats for creating a breach of security are many. The proper response to such an incident is related to the degree of impact. Iowa State University has three formal committees that have procedures in place to address many of these threats. The Critical Incident Response Team (CIRT) is a functional unit which will provide timely, comprehensive and accessible support services during critical incidents. CIRT will address critical incidents broader than major security breaches, but it would be called upon in the event of a major security breach that would have significant impact to the University. It has broad campus representation.

   The Network Incident Response Team (NIRT) is comprised of staff from Academic Information Technologies and Telecommunications. NIRT is focused on maintaining the integrity of the network infrastructure which includes the flow of information to and from the Internet.

   Administrative Technology Services has a formal disaster recovery document and a team that is assigned to respond to any incidents. The primary purpose is to address physical disasters, but due to the skills represented on the team it would also respond to serious security breaches relating to loss of information. The team has established relationships with other units on campus including the Department of Public Safety, Environmental Health and Safety, FP&M, Academic Information Technologies, and Telecommunications.

   The audit recommends expanding the formal procedures to include breaches of information security.

   The ISTF has identified as part of the process of drafting a campus security policy the need for a document that addresses the responsibilities and procedures for identifying and reporting security breaches. As this document is being drafted and reviewed by other campus administrators, an evaluation will be made as to the need for another group to respond to breaches related to information security or if the groups and procedures already in place are sufficient.

   Conclusion – Response accepted.

4) Automatic Log-off – Users should be automatically logged off by the system after a period of inactivity in order to strengthen logical controls over data files and software programs.

   Users that fail to log-off are only logged off by the system each night at 7:00 p.m.

   Recommendation – The University Administrative Technology Services Department should establish controls to automatically log off users after a preset period of inactivity.

   Response – Users of web-based AccessPlus applications are currently logged off after a period of inactivity. The time period varies for different AccessPlus applications and classes, or categories, of users. Also, Administrative Technology Services strongly encourages the use of password protected screen savers when people are away from their workstations. While some clients using our ISUAS/ADIN terminal based applications complained about the inconvenience caused by automatic logoffs when they were implemented in the past, we agree with the value and added security of such a control. Effective October 1, 2003, an automatic logoff after four hours of inactivity will be implemented for all ISUAS/ADIN terminal based production applications.

   Conclusion – Response accepted.

5) System Access for Terminated or Transferred Employees – IT Security should be notified immediately when system users are terminated or transferred in order to prevent unauthorized access to system resources.

   Iowa State University has not implemented University-wide policies and procedures to ensure that IT security is notified when employees terminate or are transferred. Also, a periodic review of those with system access is not done to determine if access is appropriate. Finally, 6 of 10 inactive user ID's tested were found to have unnecessary or inappropriate access to the ISUAS/ADIN system.

   Recommendation – The University should develop and implement procedures to ensure that IT security is notified when employees terminate employment or are transferred within the University to ensure that their system access is appropriate. Also, procedures should be put in place to periodically review those with system access to discover any improprieties.

   Response – Administrative Technology Services is aware of and has been working with campus data stewards on this issue. We will continue the efforts that are underway. Our goal is to have procedures implemented by the end of fiscal 2004 that will improve network and system access controls for ISU employees who either terminate employment or move/transfer to another department.

   Conclusion – Response accepted.

6) Promotion of Programs to Production – A programmer may check out a program, change the program, and place the program back into production. This activity is logged at the University Administrative Technology Services Department by the Source Control System utility, and a report is sent to supervisors each day of the programs checked in.

   Manager approval is not required before a program is placed into production, and no separate independent group moves programs from test to production. Also, there are no procedures in place to ensure that the log created by the Source Control System utility is routinely reviewed; therefore, unauthorized program changes could be implemented without management oversight.

Recommendation – The University Administrative Technology Services Department should implement procedures to ensure proper segregation of duties between programmer, manager sign-off, and promotion to production.

Response – Administrative Technology Services has implemented a number of significant program (software) source controls in the past several years. An automated and auditable log of all program changes is maintained which collects: 1. The person making the change, 2. The date of the change, 3. The person or process requesting the change, 4. The method of communicating the request for the change, 5. The reason or justification for the change, 6. A before and after audit trail of every line of code being added, deleted, or changed, and 7. The creation and retention of a program version with every change moved into production. An automated electronic notice containing the above information is sent to Administrative Technology Services managers daily informing them of every program being moved into production. The daily notices are permanently archived. An electronic e-mail notice sent by the analyst further documenting every program change is also required and permanently archived. An Administrative Technology Services staff person has been assigned the responsibility of doing monthly spot checks to verify the confirming e-mails were sent. In addition, source code authorizations are assigned to every program. This means that the individuals granted authorization rights to a specific program are the only individuals who can checkout, change, and check a program back into the production source code library. We believe these controls provide ample evidence of our commitment to the importance we put on the integrity and reliability of the software for which we are responsible. We also believe these controls provide a strong deterrent and do include a significant degree of management oversight. As such, including an additional manager sign-off step into the process of moving new software and software changes into our production environment would do little to strengthen the controls and would actually lengthen and slow down our ability to quickly respond to software change needs. We will continue to look for practical and effective ways to further improve and strengthen this process.

Conclusion – Response acknowledged. Procedures should ensure that only approved program changes are placed into production.

Application Controls:

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

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Gina L. Cunningham, CPA, Senior Auditor
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Travis J. Davis, CPA, Senior Auditor
Cory A. Warmuth, CPA, Staff Auditor
Julie L. Lyon, CPA, Staff Auditor
Sarah M. Wright, Staff Auditor
Matthew J. Affinson, Assistant Auditor
Curtis J. Schroeder, Assistant Auditor