



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

FOR RELEASE _____ November 30, 2010

Contact: Andy Nielsen
515/281-5834

Auditor of State David A. Vaudt today released a report on a review of selected general and application controls over the Iowa State University of Science and Technology (Iowa State University) Accounts Receivable System for the period of March 29, 2010 through May 6, 2010.

Vaudt recommended Iowa State University update and test its disaster recovery plan, ensure the Accounts Receivable Office completes the business impact analysis and implementation of its emergency plan and work with the Vet Pathology Department and Parking Division to ensure segregation of duties are established to the extent possible. The University has responded positively to the recommendations.

A copy of the report is available for review at Iowa State University, in the Office of Auditor of State and on the Auditor of State's web site at <http://auditor.iowa.gov/reports/1161-8020-BT01.pdf>.

###

**REPORT OF RECOMMENDATIONS TO
IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY
ON A REVIEW OF SELECTED GENERAL AND
APPLICATION CONTROLS OVER
THE UNIVERSITY'S ACCOUNTS RECEIVABLE SYSTEM**

MARCH 29, 2010 THROUGH MAY 6, 2010

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

October 25, 2010

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, 2010, we conducted an information technology review of selected general and application controls for the period March 29, 2010 through May 6, 2010. Our review focused on the general and application controls of the University's Accounts Receivable System 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 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 Receivable 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 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 University's Accounts Receivable System are listed on page 8 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 Chester J. Culver, Governor
Richard C. Oshlo, Jr., Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

March 29, 2010 through May 6, 2010

Accounts Receivable System General and Application Controls

A. Background

The accounts receivable system at Iowa State University (University) is used to record charges and payments to the accounts of ISU customers (the general public, staff and 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 University's accounts receivable system for the period March 29, 2010 through May 6, 2010. Specifically, we reviewed the general controls: configuration management and contingency planning, and the application controls: access controls, segregation of users, contingency planning, interface controls and business process controls, including input, processing and output. We interviewed University staff 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 which 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 which 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.

March 29, 2010 through May 6, 2010

General Controls

- (1) Disaster Recovery Planning – Disaster recovery plans are designed to help ensure an entity remains functional in the unlikely event of a loss of facilities or personnel. These plans should be updated regularly, be periodically tested, be distributed to key individuals and be maintained in written form at an off-site location. The University has prepared a disaster recovery plan for its IT systems, but the main section has not been updated since 2004 and the appendices have not been updated in over a year. In addition, the plan has not been tested with a full walk through of a disaster situation.

Prior Recommendation – The University should update its disaster recovery plan 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.

Prior Response – IT Services embarked on a comprehensive disaster recovery plan for all its buildings and units two years ago. The IT Services work group developing the plan are scheduled to meet weekly and recently completed work on drafting an Emergency Operations/Response Information template using NFPA 1600 standards. Each of the four IT Services facilities are now completing this template for their facility. The work of this group has centered on the overall disaster recovery structure for IT Services. They are doing planning preparation for a disaster response, including detailed action plans should a disaster occur. Aside from these discussions, the IT Services Data Center Operations Manager and ASB Site Coordinator are reviewing and updating the computer operations recovery documentation this year to ensure all information is up-to-date.

Current Status – Group continues to meet weekly to develop plans using NFPA 16090 standards.

Current Recommendation – We continue to encourage the University to complete its Disaster Recovery Planning.

Current Response - IT Services continues to focus on a standard disaster recovery plan format for all units within IT Services. That group is scheduled to meet weekly. In addition, another group, ASB Central System Disaster Recovery Group, has now been formed and is scheduled to meet monthly to review and update the appendices to the ASB computer operations recovery documentation. Progress will be made on both fronts in the year ahead.

Conclusion – Response accepted.

Application Controls

- (1) Emergency Planning – Emergency plans are designed to help ensure an entity remains functional in the unlikely event of a loss of facilities or personnel. These plans should be updated regularly, tested periodically, distributed to key individuals and maintained in written form at an off-site location. The Accounts Receivable Office has prepared an Emergency Plan. However, it is not

Report of Recommendations to Iowa State University

March 29, 2010 through May 6, 2010

tested annually, at least via a walk through. Also, when it was last tested, no documentation was maintained. Additionally, the Emergency plan is missing the following key details:

- A list of vendor contacts for supplies and equipment.
- A list of supplies and equipment needed to get up and running.
- A provision for annual review, updating and testing.
- Provisions for continuity if ITS is down.

A key element in the Emergency planning process is conducting a business impact analysis to identify the critical functions performed by the application and the specific IT resources required to perform the functions. The Accounts Receivable Office has conducted a Business Impact Analysis. However, it has not been completed and approved. It is still in draft form, dated January 26, 2007.

Recommendation – The Accounts Receivable Office should complete the Business Impact Analysis and implementation of its Emergency plan and distribute it to all individuals who are expected to play a key role if the plan is put into action. The plan should then be reviewed for possible updates and tested on an annual basis.

Response – The Business Impact Analysis (BIA) and Emergency Plan (EP) mentioned have been completed and submitted to ITS for review and approval. The Accounts Receivable Office will follow up to ensure approval has been obtained and will continue to review and test plans yearly. Each plan will have an Activity Log for documentation and evaluation which will state employee, system, activity and evaluation of success or failure. A listing of outside vendors for the Accounts Receivable Office will be included in the BIA and distributed to affected employees for testing purposes. The Accounts Receivable Office will critically review each annual test with programming staff from ITS, external collection agencies and billing services.

Conclusion – Response accepted.

- (2) Independent Review of Deleted Cases and Voided Tickets - Work responsibilities should be segregated so one individual does not control all critical stages of a process. In offices where segregation of duties is not possible, compensating controls should be implemented.

The Vet Pathology Department has two individuals who invoice case files daily and have the ability to delete cases. No compensating controls currently exist to have an independent person review the deleted cases.

The Parking Division is able to void tickets on the Ticket Track system. While the voided tickets are kept on file, no independent review or other compensating control is performed to ensure voided tickets are appropriate.

Report of Recommendations to Iowa State University

March 29, 2010 through May 6, 2010

Recommendation - The Controller's Department should work with the Vet Pathology Department and the Parking Division to ensure segregation of duties is established to the extent possible. If staff resources do not allow for this, a process to periodically conduct an independent review of deleted cases or voided tickets should be implemented. The Controller's Department should also consider strengthening guidance to University selling departments to ensure segregation of duties is maintained.

Response - Accounts Receivable Office Staff responsible for training for the University Receivable System (UR) have incorporated segregation of duties and departmental review in their documentation and training materials. The document provided to new UR users, Guidelines for Direct Entry and Reconciliation of Activity, discusses those duties. However, we can only ensure proper system access and not supervisor approval. We will strengthen our training regimen with regards to segregation of duties. We will also collect and retain the supervisor's name who will be responsible for review. Each year during our system access review period, we will review the documentation and strengthen our commitment to segregation of duties and independent review whenever possible. Employees will be required to verify compliance in order to continue to use the UR system.

The Controller's Department will work with the named departments to ensure adequate segregation of duties exists. The Controller will provide guidance to the campus community on the necessity of maintaining segregation of duties and/or compensating controls in an environment of reduced staffing.

Conclusion - Response accepted.

Report of Recommendations to Iowa State University

March 29, 2010 through May 6, 2010

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Patricia J. King, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Janet K. Mortvedt, CPA, Staff Auditor
Adam D. Steffensmeier, Staff Auditor
Daryl L. Hart, Assistant Auditor