OFFICE OF AUDITOR OF STATE
STATE OF IOWA

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834   Facsimile (515) 242-6134

David A. Vaudt, CPA
Auditor of State

NEWS RELEASE

FOR RELEASE   November 30, 2007

Contact: Andy Nielsen
515/281-5834

Auditor of State David A. Vaudt today released a report on the review of selected general and application controls over the State University of Iowa (University of Iowa) PeopleSoft General Ledger system for the period June 4, 2007 through July 27, 2007.

Vaudt recommended the University of Iowa develop and implement procedures to improve information system controls related to access controls, program customizations, segregation of duties and supervisory approvals.

A copy of the report is available for review at the University of Iowa, in the Office of Auditor of State and on the Auditor of State's web site at http://auditor.iowa.gov/reports/reports.htm.

# # #

REPORT OF RECOMMENDATIONS TO THE
STATE UNIVERSITY OF IOWA
ON THE REVIEW OF SELECTED GENERAL
AND APPLICATION CONTROLS OVER
THE UNIVERSITY'S PEOPLESOFT GENERAL LEDGER SYSTEM

June 4, 2007 through July 27, 2007

=== 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

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834   Facsimile (515) 242-6134

David A. Vaudt, CPA
Auditor of State

October 1, 2007

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

   In conjunction with our audit of the financial statements of the State University of Iowa (University of Iowa) for the year ended June 30, 2007, we conducted an information technology review of selected general and application controls for the period June 4, 2007 through July 27, 2007. Our review focused on the general and application controls of the University's PeopleSoft General Ledger 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 PeopleSoft General Ledger 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 the University of Iowa, citizens of the State of Iowa and other parties to whom the University of 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 of the PeopleSoft General Ledger system are listed on page 7, 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
      Charles J. Krogmeier, Director, Department of Management
      Dennis C. Prouty, Director, Legislative Services Agency

PeopleSoft General Ledger General and Application Controls

A. <u>**Background**</u>

PeopleSoft General Ledger, along with various journal entry applications, at the University of Iowa (University) are used to accumulate information for use in preparing financial statements.

B. <u>**Scope and Methodology**</u>

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 PeopleSoft General Ledger system for the period June 4, 2007 through July 27, 2007. 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 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 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. <u>**Results of the Review**</u>

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.

<u>**General Controls**</u>

(1) <u>Password Controls</u> – User ID's and passwords are used to identify and authenticate users in controlling access to system resources. Passwords, however, are not conclusive identities of specific individuals since they may be guessed, copied, overheard or recorded and played back. Typical controls for protecting the confidentiality of passwords include the requirements they be changed every 60 to 90 days, not allowed to be reused and locked out after a limited number of consecutive unsuccessful attempts. Password controls over journal entry applications and PeopleSoft General Ledger could be strengthened.

<u>Recommendation</u> – The University should implement security features to strengthen password controls for journal entry applications and PeopleSoft General Ledger.

Response – The University will implement stronger password controls and an authentication audit strategy.

Conclusion – Response accepted.

(2) System Access – Access to the journal entry application and the PeopleSoft General Ledger is assigned according to the employee's job responsibilities and needs. Authorization is granted by the employee's department head/supervisor and by the application owner, Accounting Services. The following instances were noted where procedures did not appear to be effectively restricting access according to management's wishes:

   a) Authorization forms were not on file for 29 employees with access to the General Ledger Journal Entry (GLJE) application

   b) Forms were not on file for 5 employees authorizing changes in their level of access to PeopleSoft General Ledger.

   c) Access rights for 27 employees to GLJE were not removed in a timely manner after they terminated employment or transferred to another department.

   d) Access for one employee to PeopleSoft General Ledger was not removed in a timely manner after transfer to another department.

   e) One person, who was no longer a University employee, was granted access to GLJE when the application was implemented.

   f) Two employees were granted PeopleSoft General Ledger roles different than authorized by Accounting Services.

   g) Access rights are not periodically reviewed for the journal entry applications and PeopleSoft General Ledger.

   Recommendation – Procedures should be implement to ensure access rights granted are in accordance with management's authorizations and remain appropriate for the current job responsibilities and needs of the employee.

   Response – We have reviewed all current access rights to PeopleSoft General Ledger and determined that current access rights are appropriate for job responsibilities and needs of employees. In the future, the University will improve record retention procedures and practices for authorization documents, timeliness of implementing security changes, procedures for verifying roles granted to new users and will implement a process for periodic review of access rights for all users of Journal Entry Applications and PeopleSoft General Ledger.

   Conclusion – Response accepted.

(3)   PeopleSoft General Ledger Customization – Several customizations have been made to the PeopleSoft General Ledger since implementation in January 2006. The University follows the PeopleSoft Functional Design Document (FDD) methodology for these customizations. Approval by the resource owner for movement of customization into production has not been documented.

 Recommendation – The University should take steps to ensure required procedures are followed and documented for customizations to maintain accountability.

 Response – Customizations have been reviewed with and verbally approved by Accounting Services staff. In the future, the University will extend its formal approval process to include functional approval (written sign-off of FDD) to migrate customization into production.

 Conclusion – Response accepted.

(4)   Segregation of Duties – One employee with administrative access to PeopleSoft General Ledger has gatekeeper responsibilities for placing fixes and customizations into production and also functions as the backup person to set up employee access rights.

 Recommendation – The University should take steps to ensure adequate segregation of duties relating to the PeopleSoft General Ledger is maintained.

 Response – The University is in the process of transitioning primary fix application and oversight responsibilities to a new staff member. Given the small number of PeopleSoft Functional and Technical support staff, it is difficult to maintain redundancy and complete segregation of responsibilities. To compensate for this the University will implement compensating auditing processes.

 Conclusion – Response accepted.

Application Controls

(1)   Journal Entry Approval – Journal entries should be reviewed and approved by supervisory personnel in order to ensure only authorized transactions are entered into the system. The University does not have a policy requiring review and approval of journal entries by supervisory personnel, nor do the various journal entry systems have a mechanism in place to document supervisory approval.

 Recommendation – The University should implement policies and procedures to ensure supervisory approval of journal entries is obtained and documented.

 Response – The University will implement a process to ensure and document approval of journal entries by utilizing the existing Workflow electronic approval system. This process will focus on journals prepared and submitted by individuals throughout campus. The major subsidiary systems (Payroll, A/P, Asset Management, etc.) currently require approval of transactions prior to journal generation; therefore, they will not be included in this new approval process. Other subsidiary systems will be investigated to determine the feasibility and need for inclusion in the approval process.

 Conclusion – Response accepted.

<u>Staff:</u>

Questions or requests for further assistance should be directed to:

    Erwin L. Erickson, CPA, Director
    Gwen D. Fangman, CPA, Senior Auditor II
    Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated in this review include:

    Daniel L. Grady, Senior Auditor
    Carrie L. Livingston, CPA, Staff Auditor
    Bradley A. Meisterling, Staff Auditor