ERP Position Paper #3

Date: June 11, 2004

Topic: Application Access and Security

The designing of business processes involves many decisions taken in connection with external requirements, organizational culture, and carefully balanced costs and benefits. In all business processes, efficiency together with accuracy, validity, completeness, proper authorization and documentation are key control objectives.

As internal auditors, our implementation review role includes the identification of opportunities and control concerns that need to be addressed campus-wide and by project management team. This is our third position paper and has an emphasis on application access and security. This and the other ERP position papers are accessible at:

http://oacr.ufl.edu/ERP_Position_Papers.htm

With the University's implementation of PeopleSoft applications (Bridges), many business functions will be further decentralized with after-the-fact oversight by the central processing areas. This requires that additional controls be implemented at the unit level to help safeguard university assets, ensure proper recording of transactions, provide for efficient and effective accomplishment of goals and objectives, and to ensure compliance with university rules and objectives and other governance.

Unit directors need to be fully aware of the changes in applications and their impact on key control objectives. We are concerned that most communications on these issues and training efforts may not have received sufficient attention from Deans, Directors, and Department Heads who have the budgetary and administrative authority and are accountable for financial and human resources within their units.

It is NOT Business as Usual

With the change from the existing accounting information system (FLAIR) to the new transaction coding using chart-fields to replace departmental accounts (organizational codes) and object codes, the opportunity for errors to occur and not be detected timely is significantly greater.

Although there are edits within the implemented applications to ensure that only valid chart-field combinations can be input, the financials modules as implemented do not limit the valid chart-field combinations an employee can impact.

ERP Position Paper #3
Date: June 11, 2004
Topic: Application Access and Security

Any one of the more than 1500 employees with the roles of "initiator" and "approver" may process transactions either charging an expense or crediting revenue to any unit or unit/project of the University as long as the chart-field combinations are valid.

As a compensating control, after-the-fact and sampling based reviews will be conducted by the University Controller's Office. Transactions with pre-defined attributes will be followed up as considered appropriate. Relying on post-transactional controls is less effective than front-end access restricting controls. Frequently, it takes more resources to investigate and correct errors and/or recover losses than it would take to prevent them. It is important for the University community to be aware of the wide access available to all initiators and approvers within the newly implemented system. Unit managers should initiate a more hand-on approach in the management of resources under their oversight to avoid unauthorized transactions.

It is necessary that departmental managers (supervisors for employees initiating transactions) review appropriate reports of transactions such as departmental ledgers and project ledgers, in sufficient detail to ensure that transactions are properly recorded and charged to correct chart-fields.

Training should be provided to departmental personnel on the reports available, how to read them and how to detect chart-field errors.

Delegations of authority and monitoring responsibility to staff should be very deliberate and based on an evaluation of the type of transactions and other responsibilities assigned to an employee.

Managing and Delegating Access and Authority

One of the strongest controls in any business operation is the assignment of roles and responsibilities. In PeopleSoft, the process and the roles assigned are critical to ensure that appropriate employees initiate and approve transactions with adequate separation of duties. An employee's assigned roles determine what he/she can see and do in the business processes. Although, the actual entry of role assignments is centralized in the UF Bridges Security Team, it will be dependent on requests by departments to assign specific roles to their staff.

Considering the importance of role assignments and the continuous nature of managing role-based security, we are concerned that its oversight and management is not well defined with clear lines of authority and responsibility at both the University and unit levels.

The first step is for Deans, Directors and Chairs, to assign the role of Department Security Authorizer (DSA) or to assume this role themselves. The person in this role will assign all the other roles without additional department or college review unless a process is established within the unit. This is a change from the previous process which required that the deans, directors, and chairs, approve all role assignments.

Training on the duties and significance of the new DSA role has not been emphasized and restrictions or suggestion on who should be the DSA or the number of DSA's per unit have not been provided. The Security Team will review on a case by case basis any assignments that would give a single employee incompatible roles. Although training is strongly recommended prior to being assigned roles, due to time constraints, it has not been made mandatory.

The Bridges implementation is a monumental undertaking and there are many challenges and adjustments ahead. The manner in which it is implemented at the University of Florida uses the basic premise of decentralized transactional processing and oversight. This requires that University administrators actively participate in delegation decisions and evaluate the implications of these decisions.