AUDITOR GENERAL

WILLIAM O. MONROE, CPA

UNIVERSITY OF SOUTH FLORIDA

FUNDAMENTAL ACCOUNTING SYSTEM

Information Technology Audit

SUMMARY

The University of South Florida utilized the PeopleSoft enterprise resource planning (ERP) application software for both its human resource management and financial management solutions. The applications operated within a client-server Internet-based environment supported by the University's Division of Information Technologies (ITD), organizationally placed under the Executive Vice-President and Chief Financial Officer (CFO). In conjunction with Academic Computing Technologies (ACT), ITD operated the University's backbone data network. In addition to supporting University technology systems, ITD operated the Central Florida Regional Data Center, which provided services for other educational and governmental organizations. ACT, organizationally placed under the University Provost, provided computing resources and services to the University community in direct support of instruction and research.

Our audit focused on the University's PeopleSoft Financial System, referred to as the Fundamental Accounting System (FAST), including an evaluation of selected general and application information technology (IT) controls applicable to FAST during the period July 2004 through October 2004. We also evaluated University actions taken in response to selected IT-related deficiencies noted in audit report No. 2004-022.

As described below, we noted deficiencies in University management controls over selected IT functions and practices.

<u>Finding No. 1:</u> The University did not have an adequate IT security management structure in place to formally develop and implement a security program for the University community.

<u>Finding No. 2:</u> Deficiencies were noted in the University's procedures for restricting access to appropriate users.

<u>Finding No. 3:</u> Various other deficiencies were noted in general and application controls surrounding FAST.

BACKGROUND

The University transitioned from the State's financial and accounting system, the Florida Accounting Information Resource Subsystem, to FAST on July 1, 2003. The University obtained PeopleSoft's Financial System due to its seamless integration with the University's installed PeopleSoft Human Resource

Management System, familiarity with system look and feel, and the ability to leverage the infrastructure, database, and technical knowledge previously gained. Modules used within the Financial System application included accounts payable, commitment control, general ledger, grants management, purchase order, asset management, accounts receivable, billing, and project costing. Users accessed FAST via a Web browser. Application security was based on display, add, and update actions allowed on the individual display and data-entry screens, referred to as pages. Permission lists controlled page-level access with users inheriting permissions by way of one or more roles assigned to their user profile. A limited number of users had been granted direct database sign-on privileges for broader reporting capabilities than provided through the application's reporting tool.

Finding No. 1: University Security Structure

Enterprise information resources and systems are shared resources requiring security and management strategies to be coordinated across the enterprise. An entitywide program for security planning and management is the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. Principles needed to ensure the information security program addresses current risks include establishing a sound IT risk management process to identify, assess, and mitigate risks; implementing and communicating appropriate policies and controls; promoting security awareness; and monitoring the effectiveness of the policies and controls. Assigning responsibility for securing information assets to a designated information security manager who is placed at a sufficiently high level within the organization promotes an effective and efficient security structure and framework that supports the development of and compliance with security policies, procedures, and guidelines.

While the University had charged the Associate Director of Systems Operations for ACT with Universitywide security responsibilities, the scope and authority of these duties had not been formally defined. Accordingly, reports and recommendations issued under this role were not necessarily viewed as management directives. Further, proposed security initiatives required consensus across several Vice-President administration levels, including the CFO, Provost, and Vice-President for Health Sciences, with security solutions organizationally funded when deemed necessary. Deficiencies were noted in the coordination and facilitation of a formal, unified University security program as follows:

- Although ITD had developed a risk assessment for its defined areas of responsibility, a comprehensive security risk assessment, wherein vulnerabilities, acceptable levels of risk, and mitigation factors were identified, had not been conducted at a Universitywide level in order to commit funding sources and policy to achieving security solutions and measures.

- Security policies and best practices associated with colleges' and departments' use and protection of microcomputing resources and the general appropriate use of IT resources were available on the University's Web site; however, most existed as drafts, suggestions, in progress, or were not reflective of the current environment, rather than University approved and imposed policy.
- Security policies, including University, College, Campus, and departmental policies regarding data access, consequences of security breach, and incident response procedures, were not effectively communicated to employees through an on-going awareness training program. Although access requests to the business enterprise applications incorporated a signed statement of responsibility, employees did not periodically renew a signed statement of understanding and accountability for securing granted access to IT resources and data.

The current organizational placement of the information security management responsibilities, together with a lack of clear definition of the scope and authority of the function, may not provide sufficient oversight of and emphasis on the importance of information security at the University. As a result, the effectiveness of information security could be limited.

Recommendation: The University should reposition the security management function to strengthen its authority and independence and foster a formal, unified security program for all University information resources. The security program should incorporate a systematic Universitywide security risk assessment framework through which appropriate policy will be developed, funded as applicable, enforced through education and accountability, and consistently re-evaluated in response to developing situations.

Finding No. 2: Access Authorization

Proper restriction of system access to authorized individuals permits user access to application software processing functions solely for purposes of performing assigned duties and precludes unauthorized persons from gaining access.

Our audit disclosed instances of inappropriate or unnecessary system access privileges, as noted below:

- A data utility and action type had not been appropriately restricted. During our audit, we noted that nine user roles had been granted access to the Data_Mover menu. Data_Mover is a data management tool used to transfer data between databases and platforms, such as between development and test environments, or to update system tables, such as for applying application upgrades. The extension of system utility privileges to the end user community exposes the system to unauthorized changes which may not be timely detected. Additionally, a key control over security administration includes specific policies and procedures on the use and assignment of the correct history action type. Correction mode access allows the alteration, insertion, or deletion of data rows regardless of the data's effective date and without the creation of an audit trail. Consequently, as data integrity and management reporting from the system may be adversely affected, correction mode access is intended to be granted under limited and monitored circumstances. Our audit noted that 1,885 users had been granted correction mode access. The extension of correction mode in mass severely diminishes the University's ability to detect, identify, and subsequently investigate inappropriate changes.

Subsequent to our fieldwork, ITD indicated that Data_ Mover menu access had been reviewed and removed from user roles as deemed appropriate.

- Clear division of roles and responsibilities between IT development staff and functional end users as well as within the established overall IT function is a key element of internal control to exclude the possibility of a single individual subverting a critical process. For example, the functions of application end user, application development and maintenance, and technical (systems software) support are typically segregated. Additionally, as resources permit, it is generally advisable to limit technical support staff's access privileges to the software products for which they are responsible. Our audit noted that ITD technical support staff maintained all application rights through granted access via one or more roles to the ALLPAGES permission list, which provided full access to all administrative and functional related pages within FAST. Further, staff were assigned additional roles which duplicated the ALLPAGES access. These roles were not assigned to any other users. Additionally, ITD technical support staff maintained overlapping capabilities within the supporting network, database, and server operating system components of FAST with some staff having full access rights on all platforms in addition to the FAST application. Inadequate segregation of duties may result in improper system changes, erroneous transactions processed, or damage to computer and information assets.

  Subsequent to our review, ITD management acknowledged that certain personnel must maintain substantial access privileges and, in response, indicated that it is developing a code of conduct for data integrity to be signed by all personnel.

- Termination procedures are developed and responsibilities assigned to specific departments in an organization to ensure timely notification to the data security administrator function of change in employee status and cancellation of access privileges to critical areas, specific data systems, and the installation as a whole. The University did not have a current, formal procedure in place to ensure the timely notification of and deletion or deactivation of user accounts for terminated or transferred employees. During the fiscal year ending June 30, 2004, 15 administrative employees were terminated. Four of those employees retained FAST accounts. Of the four accounts, one had been locked with the other three accounts continuing active status. Our test results further revealed that none of the users had actually used the account prior to or subsequent to termination. Without adequate procedures to ensure the timely revocation of access, the risk is increased of unauthorized access to University information resources.

Recommendation: In order to preserve the integrity, confidentiality, and availability of its information resources, the University should strengthen access authorization controls in the above-cited areas. Specifically, users' roles should be reviewed to ensure that they are reflective of the job duties of the individual to whom they are assigned and correction mode access should be granted based on defined circumstances and responsibility. Additionally, management should critically evaluate and define the system and database administration roles and responsibilities of each ITD technical support staff member with regard to the supporting network, operating system, and database platforms. Update access through FAST application sign-on should not be a function of technical staff. Roles should be created as required for functionality and accordingly assigned respective of technical job duties stipulated. Further, the University should develop detailed procedures, including departmental and personnel assignment, necessary to ensure that all terminated or transferred employees' access rights are timely revoked.

Finding No. 3: Application Environment and Support Functions

Security considerations for all components of a system environment, including application, operating system, network, and physical levels, contribute to the reliability and integrity of the applications and data processed therein. Developing and maintaining procedures to ensure the proper use of the application, data management, and technological solutions put in place is enabled by a structured approach to the combination of general and application controls over IT operations. Well documented policies and procedures describing the scope of the IT function, activities, and interrelationships with other departments establish direction and implementation measures as well as contribute to an effective control environment.

Deficiencies were noted in general and application controls surrounding FAST.

- We noted certain control deficiencies in the FAST environment related to system logging, password and user workstation controls, business continuity plan validation, wireless access, and database security controls. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising University information. However, appropriate University personnel have been notified of the deficiencies.
- Informal procedures existed and were executed in the daily course of ITD's support of FAST. However, formally defined policies and procedures,

including delegation of authority and responsibility, had not been developed to adequately govern user access issuance; network monitoring and incident response measures; and database and server operating system administration. Further, network maintenance procedures, including firewall, intrusion detection system, and virus software management; and system software, including switches and routers, upgrade, patch, and maintenance procedures had not been formally defined. Without formal policies and procedures outlining controls and measures necessary for the quality and consistency with which an entity's objectives are achieved, management cannot be assured that personnel have the appropriate guidance for performing directives in accordance with expectations.

- Validation and editing close to the point of origin ensures accuracy, completeness, and validity of transaction data entered for processing. During our audit, University staff indicated the vendor and manufacturer name and data prompt edit controls were not in use. Consequently, users could create multiple entries of the same vendor or manufacturer rather than associating multiple addresses for one vendor or manufacturer name. The lack of edit controls poses difficulties in reporting and reconciling procedures and, in time, could increase data clean up and conversion efforts. Subsequent to our audit, ITD indicated that these edits are planned for implementation.
- As ERP implementations bring fundamental changes in control methods, point of control, and control level, considerable staff training is required to adapt to new processes and systems. Adequate training focuses on the system's use in daily practice. During our audit, project management staff noted areas of training which could be improved, including budget and expenditure transfers and follow-up or error correction, reconciliation between central and departmental level modules, budget checking, year-end procedures, available reporting, general ledger feeder module, and security. Inadequate training may result in incorrect end user processes, inefficient or ineffective use of resources, and additional time and effort spent correcting errors or omissions.

Recommendation: University management should strengthen its controls surrounding the FAST environment through developing a complete and comprehensive set of policies and procedures addressing ITD responsibilities noted above; implementing system edit controls designed to reduce data duplication; and implementing comprehensive training courses for all critical business areas. Training should be directed to both new and continuing employees to enforce business processes related to their functional responsibilities and should provide a mechanism for follow-up activities to timely resolve frequent processing errors or issues.

PRIOR AUDIT FINDINGS

The University had corrected, or was in the process of correcting, portions of the IT-related deficiencies noted in audit report No. 2004-022. Certain issues within Finding No. 3 were previously reported and remain unresolved.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected University IT controls and to determine the steps taken in response to selected IT-related deficiencies noted in audit report No. 2004-022. Our scope focused on evaluating selected general and application IT controls applicable to FAST during the period July 2004 through October 2004. In conducting our audit, we interviewed appropriate personnel, observed University processes and procedures, and performed various other audit procedures to test selected IT controls.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

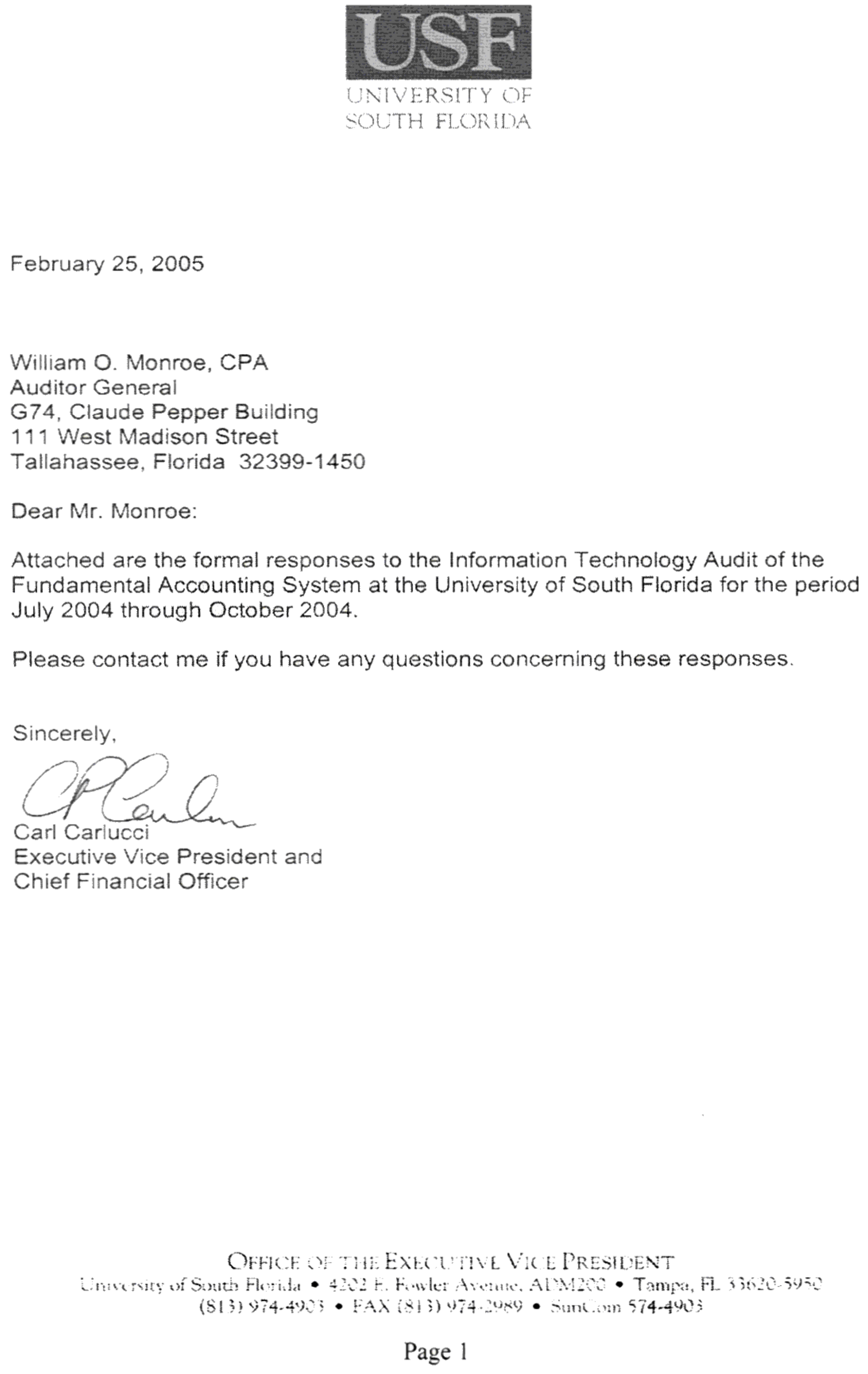
UNIVERSITY'S RESPONSE

In a letter dated February 25, 2005, the University provided responses to our preliminary and tentative findings. This letter is included in its entirety at the end of this report.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Heidi Burns, CPA*, CISA, and supervised by Nancy Reeder, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.state.fl.us/audgen); by telephone (850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.



USF
UNIVERSITY OF
SOUTH FLORIDA

February 25, 2005

William O. Monroe, CPA
Auditor General
G74, Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Attached are the formal responses to the Information Technology Audit of the Fundamental Accounting System at the University of South Florida for the period July 2004 through October 2004.

Please contact me if you have any questions concerning these responses.

Sincerely,

Carl Carlucci
Executive Vice President and
Chief Financial Officer

Finding No. 1: The University did not have an adequate IT security management structure in place to formally develop and implement a security program for the University community.

Recommendation: The University should reposition the security management function to strengthen its authority and independence and foster a formal, unified security program for all University information resources. The security program should incorporate a systematic University-wide security risk assessment framework through which appropriate policy will be developed, funded as applicable, enforced through education and accountability, and consistently re-evaluated in response to developing situations.

The University has established an information security structure in order to identify risk, implement risk mitigation strategies and programs, and provide overall coordination of security measures.
The University believes that the structure that was established to address security issues, the Information Security Officer and Information Security Workgroup, is a sound, effective approach. In review of the audit findings and recommendations, the following steps will be taken to buttress that structure.

- The policy which established the Information Security Workgroup (ISWG) and Information Security Officer (ISO) (Policy 0-508) will be updated and then formally promulgated through the proper processes of the General Counsel (the General Counsel is a member of the ISWG).
- The Information Security Workgroup will add two representatives in order to address additional areas of information security. There will be a representative of the Enterprise Business Systems and a representative of the Data Warehouse Security Team. This change will be reflected in Policy 0-508.
- The ISWG will be sponsored by and report to the Enterprise Business System Sponsors., who will be provided recommendations for policy, procedures, and resource requirements by the ISO and ISWG. This change will be reflected in Policy 0-508.

The re-constituted and reinforced ISWG will establish a formal university-wide risk assessment program. The ISWG will meet quarterly to review routine issues of policy, practice and resource requirements and will present to the Enterprise Business System Sponsors a quarterly report of its findings and recommendations. The ISWG will convene as needed to address additional issues which arise and as requested by the ISO or any member of the workgroup.

Responsible Party: George Ellis
Implementation Date: July 1, 2005

Finding No. 2: Deficiencies were noted in the University's procedures for restricting access to appropriate users.

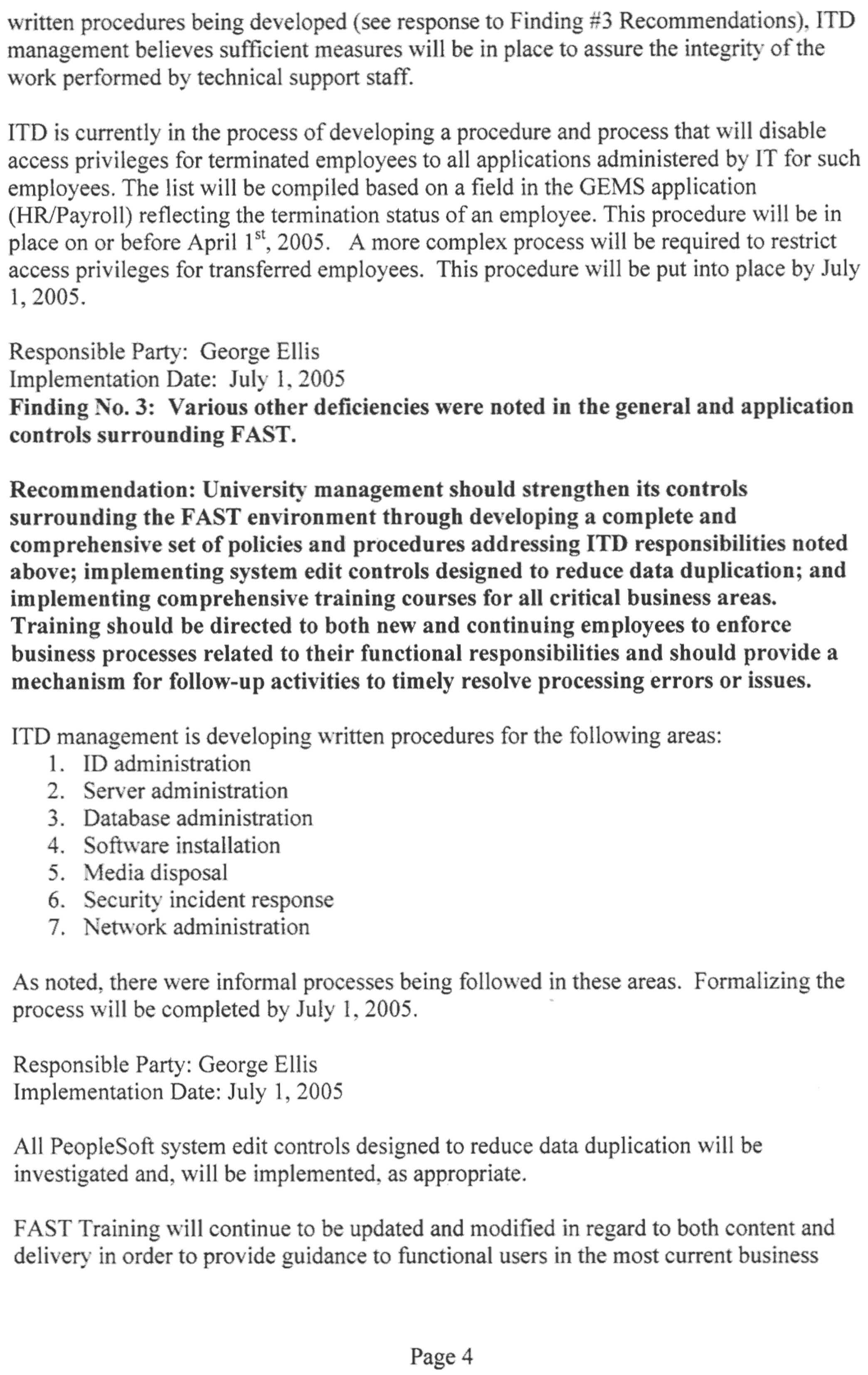
Recommendation: In order to preserve the integrity, confidentiality, and availability of its information resources, the University should strengthen access authorization controls in the above-cited areas. Specifically, users' roles should be reviewed to ensure that they are reflective the job duties of the individual to whom they are assigned and correction mode access should be granted based on defined circumstances and responsibility. Additionally, management should critically evaluate and define the system and database administration roles and responsibilities of each ITD technical support staff member with regard to the supporting networks, operating systems, and database platforms. Update access through FAST application sign-on should not be a function of technical staff. Roles should be created as required for functionality and accordingly assigned respective of technical job duties stipulated. Further, the University should develop detailed procedures, including departmental and personnel assignment, necessary to ensure that all terminated or transferred employees' access rights are timely revoked.

The University has taken steps to strengthen access controls as noted. Specifically, the Functional Project Managers (FPM) for the Enterprise Business Systems (which includes FAST), have been given the direction to review all user roles that had been established in the implementation of the systems. While the business process owners have the primary responsibility for access controls, the FPM will provide an independent, oversight function. A monitoring and oversight function has been established within the FPM organization and a staff member has been hired. This staff member will be establishing a formal process for periodically reviewing roles and permissions, including ensuring correction mode is assigned and used correctly. These assessments will be shared with the internal auditing function, as needed.

ITD management is now reviewing the roles pertaining to development and technical support staff to ensure access by these individuals is limited to the minimum required to perform their duties. Subsequent to the Auditor General's fieldwork, ITD has established a full-time security position which has been filled by an existing technical staff person. This position was established because of the need for additional attention to such issues.

ITD already separates the functions of application developer from technical support (database management and systems administration) as a means of internal control. ITD management has now reviewed the issue concerning technical support staff having administrative privileges in multiple environments (Unix, Windows, Oracle and/or PeopleSoft). ITD management has carefully assessed the risk of this practice and concluded it is not feasible to restrict a technical support member to administrative privileges in only one such environment. To add these restrictions would seriously impact problem diagnosis and resolution and implementation/activation of upgrades. However, ITD management will ensure such access is kept to the minimum required, and additional monitoring and oversight will be provided.

It should be noted ITD management has already implemented actions to reduce risk. It has required background checks on technical support personnel for several years and has now finalized a standard of behavior to be signed by all personnel. Additionally, with the



written procedures being developed (see response to Finding #3 Recommendations), ITD management believes sufficient measures will be in place to assure the integrity of the work performed by technical support staff.

ITD is currently in the process of developing a procedure and process that will disable access privileges for terminated employees to all applications administered by IT for such employees. The list will be compiled based on a field in the GEMS application (HR/Payroll) reflecting the termination status of an employee. This procedure will be in place on or before April 1st, 2005. A more complex process will be required to restrict access privileges for transferred employees. This procedure will be put into place by July 1, 2005.

Responsible Party: George Ellis
Implementation Date: July 1, 2005
Finding No. 3: Various other deficiencies were noted in the general and application controls surrounding FAST.

Recommendation: University management should strengthen its controls surrounding the FAST environment through developing a complete and comprehensive set of policies and procedures addressing ITD responsibilities noted above; implementing system edit controls designed to reduce data duplication; and implementing comprehensive training courses for all critical business areas. Training should be directed to both new and continuing employees to enforce business processes related to their functional responsibilities and should provide a mechanism for follow-up activities to timely resolve processing errors or issues.

ITD management is developing written procedures for the following areas:

1. ID administration
2. Server administration
3. Database administration
4. Software installation
5. Media disposal
6. Security incident response
7. Network administration

As noted, there were informal processes being followed in these areas. Formalizing the process will be completed by July 1, 2005.

Responsible Party: George Ellis
Implementation Date: July 1, 2005

All PeopleSoft system edit controls designed to reduce data duplication will be investigated and, will be implemented, as appropriate.

FAST Training will continue to be updated and modified in regard to both content and delivery in order to provide guidance to functional users in the most current business

processes. Particular emphasis will be placed on identifying the most frequent processing errors and incorporating a resolution for these errors within the training. Workgroups have been established to identify and prioritize staff training needs in the user community and to recommend training objectives and agendas for USF staff.

Responsible Party: Nick Trivunovich
Implementation Date: 7/1/05