



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



UNIVERSITY OF FLORIDA

PEOPLESOFT FINANCIALS SYSTEM

Information Technology Audit

SUMMARY

The University of Florida (University) utilized the Oracle-PeopleSoft (PeopleSoft) Financials and Human Resources Management System (HRMS) application suites as its enterprise resource planning (ERP) solution. The applications operated within an Internet-based environment as part of a group of integrated systems referred to collectively by the University as the myUFL systems. The myUFL systems were built, deployed, and maintained by UF Bridges, a University division reporting to the Vice President of Finance and Administration. The University's Office of Information Technology, Computing and Network Services (CNS) provided large-scale centralized computing services for the University, the University of North Florida, and other State educational institutions and agencies in northern Florida.

Our audit focused on evaluating selected information technology (IT) controls applicable to the PeopleSoft Financials System, as implemented and administered by the University, and selected internal controls related to the University's overall IT environment, for the period July 2005 through December 2005.

As described below, we noted that improvements were needed in certain controls related to the University's IT functions and practices.

Finding No. 1: There was a need for improved University level governance of the myUFL systems and the enterprise data contained therein.

Finding No. 2: Improvements were needed in segregating and limiting UF Bridges staff access within PeopleSoft Financials.

Finding No. 3: Deficiencies were noted in general and application controls surrounding the myUFL systems.

Finding No. 4: Improvements were needed in limiting access to the data center and to core network rooms located throughout the University.

BACKGROUND

The University transitioned from the State's financial accounting system, the Florida Accounting Information Resource Subsystem (FLAIR), to PeopleSoft's Financials and HRMS application software. Both systems went live on July 1, 2004. Additional systems in support of the Financials and HRMS systems were implemented prior to July 1, 2004, including PeopleSoft's Portal software, which provided a single interface for integrated systems and Enterprise Performance Management (EPM) software solution for the Enterprise Data Warehouse. To complement PeopleSoft, the University acquired Cognos business intelligence software for reporting and analysis. These integrated systems were collectively referred to as the myUFL systems.

The myUFL portal provided a single credential sign-on point of entry to the enterprise business systems for faculty, staff, and students. Additionally, the portal provided accessibility to University news, information updates, services, including password management, and legacy systems. As of the completion of our audit field work, a project to implement the PeopleSoft Student Administration System as an integrated

component of the myUFL systems had been postponed to an unspecified point in time.

UF Bridges was formed as a University division spanning a multi-year project dedicated to building, deploying, and maintaining the myUFL systems. Implementation of the systems began in the fall of 2002. UF Bridges was comprised of employees with technical and functional expertise from areas throughout campus working in concert with University staff and outside consultants to ensure the transition from legacy systems to enterprise systems. UF Bridges was structured under a Director, who also served as the Project Manager, and consisted of teams divided into key areas including, Change Control, Data Administration, Production Support Services; Enterprise Reporting; Financials; Infrastructure, Database Administration, Outreach; Human Resources Management System; PeopleSoft Development; Student Financial Application; and Grants. Each team lead reported to the Director with the exception of the Director of Data Infrastructure responsible for Infrastructure, Database Administration, Outreach, who reported to the Associate Vice-Provost for IT. During our audit period, staffing assignments and responsibilities within and among these areas had undergone change. Over 130 staff remained assigned to UF Bridges.

Post-implementation, UF Bridges continued as the myUFL systems owner, supporting and facilitating the systems' use through development, maintenance, training, and disseminating information. Responsibilities for input, processing, and reconciliation of data output were in the process of being transferred wholly to the end users as functional owners. As such, the Director developed ongoing initiatives to effect a more stabilized transition to the myUFL systems for the University community as well as address key areas of weakness identified post-implementation. Initiatives included defining and refining roles and responsibilities of UF Bridges and those of the University community in order to exact a shared commitment of effort and resources to a PeopleSoft success strategy. Additionally, the

adequacy and appropriateness of business processes as newly defined through the myUFL systems were scheduled for review and assessment, jointly by UF Bridges team leads and University functional leads, to determine whether application modification was necessary to reflect and achieve functionality more accommodating to stated business purpose or operations. Reporting continued as a high priority with ongoing effort between UF Bridges and the core offices around campus to address outstanding needs or changes. Staff were also dedicated to the Contracts and Grants module which, according to the University, had not contained accurate data nor been fully functional since implementation. Further priority projects included identification and monitoring of key transaction screens for performance analysis and reducing the lag time of the EPM update from PeopleSoft production.

CNS, in addition to providing central computing services, maintained the campus' backbone network connecting the various buildings to one another and to the Internet and served as the central network security office safeguarding against and responding to network-based threats to the computing and communications infrastructure. The Director of CNS reported to the Associate Vice-Provost for IT, who, in turn, reported to the University Provost and Senior Vice-President. Within the University, colleges, departments, or divisions functioned as separate business operating units under their own defined security authority and responsibility.

In October 2005, we released audit report No. 2006-040, an operational audit of the University. In addition to the items discussed further in the following paragraphs, audit report No. 2006-040 also discussed policies and procedures, role assignment, data extraction and reporting, and reconciliations regarding the myUFL systems.

Finding No. 1:
**University Governance of the MyUFL Systems
 and Enterprise Data**

Enterprise information resources and systems are shared resources requiring senior management's commitment to security and management strategies coordinated across the enterprise. Security management responsibility is optimally established at the organizationwide level to deal with overall security issues in the organization. Management's ultimate objective under an enterprise governance model is to conduct day-to-day operations of the organization and to accomplish the organization's stated missions with security commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Management, through enterprise governance of IT, can provide increased assurance that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance, or operation of information systems.

UF information security roles were organized in three main levels with Level 1 having responsibility for the entire university. Level 2 roles held responsibility for units throughout the University defined as colleges, departments, research centers, institutes, or other administrative subdivisions connected to the University network and Level 3 roles were responsible for smaller units within Level 2 units, as defined by the Level 2 unit. Level 1 roles consisted of the UF Information Security Administrator (UF ISA) and the UF Information Security Manager (UF ISM). The UF ISA had the responsibility to ensure implementation and management of the University's IT security program and the authority to enforce University IT policies, standards, and procedures and to direct action related to violations. The UF ISM managed the University's IT security program and security team organizationally placed under the Director of CNS. Security authority and responsibility were defined at the unit level with Level 2 roles consisting of the Unit

ISA and Unit ISM. Unit Administrators had the option of delegating their Level 2 Unit ISA authority for managing the unit's IT security program. IT security responsibilities and reporting structure within the unit were at the discretion of the Level 2 Unit ISA, who appointed a Unit ISM. The unit ISM managed and coordinated security efforts within the unit's organizational hierarchy.

In accordance with the University's IT Data Security Standard, each Level 2 Unit ISA must ensure specific data security procedures were written for their units. The standard provided data classification guidelines, including data description, assignment of data principal (owner) and custodian, restrictions on access, protection methods for access, storage, and transmission, availability requirements, and disposal methods.

With the advent of the ERP initiative and myUFL systems, core business processes underwent significant change affecting all aspects of the management of university resources. Accordingly, enterprise information was directly accessible on-line to increased groups of people. Consequently, the importance of enterprise level management of IT, and the myUFL systems in particular, was increased.

Our audit disclosed that the following deficiencies indicate a need for improved University level governance of the myUFL systems and the enterprise data contained therein, including standardized procedures and centralized enforcement:

- The University had not conducted a risk assessment specific to the myUFL systems incorporating its architectural framework and authentication mechanisms. The implementation of an ERP system can introduce new risks and alter an organization's risk profile. Management of IT-related risks is a key part of enterprise IT governance. Incorporating an enterprisewide perspective into day-to-day governance actions helps an entity understand its greatest security risk exposures and determine whether it is secure enough to ensure enterprise viability. Risk identification and impact analysis helps support management's decisions in

establishing cost effective measures to mitigate risk and, where appropriate, formally accepting residual risk. While the University had previously contracted with Predictive Systems, Inc., for services to include multiple security program assessments for 14 specific departments as part of an overall risk assessment; the security program assessments were completed in June 2003 and did not include UF Bridges or the myUFL systems. In accordance with the University IT Security Risk Assessment policy, Unit Level 2 ISMs must ensure that IT risk assessments are performed for their units on an annual basis. However, these unit risk assessments were neither reviewed at the university level by the UF ISM nor incorporated into an overall universitywide risk framework whereby University management formally acknowledged risk factors or vulnerabilities present within the operating environment, approved mitigation measures and resources therein, and accepted and assumed accountability for any residual risk.

- The University lacked written standards for authorized transmission of the myUFL system data over emerging technologies, including wireless, Virtual Private Networks (VPN), and Voice over Internet Protocol (VoIP). Inadequate data transmission standards, including, in particular, provision for encryption, increases the risk that the transmission of administrative information over the network (or Internet) could result in unauthorized access to or modification and misaddressing of sensitive data streams.
- The University lacked defined procedures for complying with its IT Data Security Standard's policy regarding annual review of employee access. UF Bridges staff established an informal role access certification policy whereby the department (unit level) security administrator (DSA) reviewed user access by virtue of making changes or updates to the user's security profile through the access request system. Subsequent to our audit inquiries, management indicated that a means to notify a DSA when roles have not been reviewed in this manner within the last year will be developed by the end of 2006. Without written procedures in place that require a routine review of user roles and privileges, management may not be assured that authorized access continues to be appropriate and consistently enables a proper segregation of duties.
- Responsibilities of the DSAs included deleting user roles specific to the PeopleSoft application for transferred or terminated employees. While the myUFL systems sign-on account was systematically locked upon input of a termination in HRMS, written procedures were not in place to ensure the removal of user roles assigned to allow access to application functions and subfunctions, or the deletion of user sign-on accounts. As similarly noted in our audit report No. 2006-040, user roles were not always revoked upon termination. Our audit further noted that as of November 14, 2005, user roles assigned within PeopleSoft Financials remained defined for 12 out of 15 Finance and Accounting employees who terminated during the period July 29, 2004, through May 4, 2005. In response to our audit inquiries, UF Bridges management indicated that termination cleanup procedures were initiated with the DSAs with an expected completion timeframe of December 2005. Without adequate procedures to timely revoke user access, the risk is increased for unauthorized access to the University's information resources.
- Provisions for recovery of the myUFL systems, along with measures and schedules to test the recovery procedures, had not been formally documented in a written disaster recovery plan. Disaster recovery planning is an element of information technology controls established to manage the availability of valuable data and computer resources in the event of a processing disruption. Its main objective is to provide the organization a plan for continuing critical operations, and, in an IT environment such as the University's, should take into consideration the significant dependence of its business processes on the ERP system. The success and effectiveness of a disaster recovery plan requires detailed development of back-up and recovery procedures, including identification of facilities, personnel, hardware, software, communications, and support services, as well as a commitment from management. The lack of an approved and detailed disaster recovery plan may jeopardize the University's efforts to efficiently and effectively continue operations with minimal loss and processing

disruption, should an event occur that interrupts IT services.

- As similarly noted in audit report No. 2006-040, Finding No. 2, initial training was not sufficient in user completion, content, and timing. Our audit additionally noted that training for the PeopleSoft applications was not mandated by the University and did not include security awareness training for handling data and preserving its confidentiality, such as procedures for securing data downloaded to the workstation. As ERP implementations can bring fundamental changes in control methods, points of control, and control levels, considerable staff training is required to adapt to new processes and systems. An important aspect of training in an ERP implementation is the provision of a system overview and an understanding of the impact of users' actions on the process, system, and other users. In conjunction with training, change management and user awareness is a critical component for user acceptance. Training principles further include communicating appropriate security policies and controls for managing data. As of the completion of our audit field work, the University continued to offer PeopleSoft training. In response to our audit inquiry, University management indicated that training was in the process of being enhanced to include detailed coverage of system transaction flow, processing dependencies, and impact of key transaction types, including management level approvals. Although the University had published a UF IT Data Security Standard on its Web site, the standard did not detail procedures specific to the user's responsibility to protect confidential and sensitive data related to the myUFL systems. The absence of required user training for both application functionality and data security responsibility may result in incorrect end user processes, inefficient or ineffective use of resources, additional time and effort spent correcting repeated errors or omissions, and compromise of information.
- The University's IT Data Security Standard listed disposal methods as a step under Data Classification Guidelines and stated, for data classified as sensitive, that data must be rendered unreadable prior to disposal. However, the standard did not detail specific procedures or provide a link to the Asset

Management Services Web page, which provided recommended resources for software and methods for securely destroying data. Additionally, neither procedures nor specific contract provisions were in place to ensure proper disposal of confidential information remaining on media in a contractor's possession upon termination of the contract. Without effectively defining and distributing procedures by which to remove sensitive data or software from discarded or transferred computer equipment, the risk is increased that sensitive information could be recovered and inappropriately used by individuals having access to the equipment.

- Prior to selection to the implementation team, UF Bridges staff had not undergone background checks or signed confidentiality agreements in acknowledgement of performing duties related to positions of special trust. Key personnel are essential for the control of critical or sensitive IT processes. Accordingly, background checks and acknowledgement of responsibility and accountability for adherence to management policies and procedures, code of ethics, and professional practices are effective measures in assuring information security and internal control. Management indicated during the course of our audit its intention to have UF Bridges staff as well as contractors sign confidentiality agreements. Further, background checks were required of University employees hired beginning in August 2005.
- The University's Americans with Disabilities Act (ADA) Compliance Office policy provides that, under the guidelines of the ADA, the University is required to make reasonable accommodations in providing services to students, staff, faculty, or visitors with disabilities. Consistent with Title II of the ADA of 1990 and its implementing regulations¹ or Section 508 of the Rehabilitation Act of 1973, as amended² (Section 508), the University had published recommended guidelines for implementation of University Web sites. In recognition of accessibility provisions under Section 508, the University placed reliance on PeopleSoft's position of compliance with regard to its

¹ 42 U.S.C. § 12132, 28 CFR 35.149-35.150

² 29 U.S.C. § 794d

application software. The University's written change control procedures for the myUFL systems, however, did not include procedures to ensure that any changes or customizations to the application supported continued compliance with Section 508.

- A key control over security administration includes specific policies and procedures on the use and assignment of the correct history action type. In the PeopleSoft application, correction mode access allows the alteration, insertion, or deletion of data rows regardless of the data's effective date and without logging the action. 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. The University had not formally defined circumstances or designated personnel appropriate for correction usage. The extension of correction mode access to multiple users without clearly defined circumstances and responsibility severely diminishes the University's ability to detect, identify, and subsequently investigate inappropriate changes.
- In association with the ERP project initiative, staff within UF Bridges created an enterprise Active Directory. Active Directory is an operating system feature that, among other things, enables the centralized management and control of a network. The intent of utilizing the Active Directory was to enhance security and stability by facilitating best practices across management domains, and provide a cost-effective platform for future enterprise development. The University did not require the University's business unit local networks to join under the enterprise Active Directory. Therefore, the University had not capitalized on a given business strategy, increasing the potential for redundant management tasks, reduced inter-operability and isolation of systems, and increased total cost of ownership of University resources.

Enterprise security relegated to varying technical specialties within individual campus units may not achieve a sustainable capability for developing and implementing proactive measures to mitigate security problems or incidents. Without applying management and security procedures for enterprise IT resources

and data at a University level of governance, the University may fail to identify and enact security controls necessary to adequately protect information systems that support the operations and assets of the organization and, thereby, accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, provide reliable financial reporting, and protect individuals.

Recommendation: A University level governance model should be adopted to create a centralized authority for managing and securing the myUFL systems enterprise data. Based on a formal, documented risk assessment, written procedures should be initiated to address those areas noted above with consistent enterprisewide application to support the confidentiality, availability, and integrity of its information resources.

**Finding No. 2:
Application 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:

- 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 preclude 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 73 UF Bridges staff, one of whom was no longer with the project, maintained all application rights through granted access via the UFICP_ALLPAGES permission list assigned

to them, which provided full access to all functional related pages within PeopleSoft Financials. Some of the pages allowed the creation of payments, journal suspense correction, marking journals for unposting, and approving vouchers. Seven of these staff had vendor maintenance capability. During the course of our audit, UF Bridges management indicated its intention to remove this access, as appropriate, as more functions and tasks in the day-to-day operation of the application are transferred to the core end-user groups. Inadequate segregation of duties may result in improper system changes, erroneous transactions processed, or damage to computer and information assets.

- Our audit noted that two UF Bridges staff maintained access privileges to perform role and user security maintenance. As the two individuals were no longer assigned to the security team, this access was outside of their respective job responsibilities and therefore, inappropriate. In response to our audit inquiries, UF Bridges staff indicated that the access had subsequently been removed.

Recommendation: Management should critically evaluate and define the application, system, and database administration roles and responsibilities of each UF Bridges staff member and assign those roles required only for the functionality respective of the technical job duties stipulated. Update access to data directly through the PeopleSoft application should not be a defined function of UF Bridges staff.

Finding No. 3:

Application Environment and Support Function

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 the 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.

We noted certain control deficiencies in the myUFL systems environment related to system logging, password and user workstation controls, network authentication, wireless access, and operating system 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 UF Bridges support of myUFL systems. However, formally defined written policies and procedures, including delegation of authority and responsibility, had not been developed to govern user account management within AIX and DB2; network, host operating system, and database administration, including user account management, security settings, monitoring of security related events, and provision for changing system delivered IDs; maintenance of firewall (ACL) settings; and monitoring for and implementation of system software upgrades and patches, including switches and routers. Formal written policies and procedures outlining controls and measures necessary for the quality and consistency with which an entity's objectives are achieved would help provide management assurances that personnel have the appropriate guidance for performing directives in accordance with expectations or with consistent application.

Recommendation: University management should strengthen its controls surrounding the myUFL systems environment through developing a complete and comprehensive set of written policies and procedures and addressing those responsibilities noted above, including provisions for delegation of authority.

**Finding No. 4:
Physical Access Controls**

Appropriate physical security and access control measures are necessary to protect IT facilities and resources and restrict access to those individuals requiring access to perform defined job responsibilities. We noted that personnel from CNS's Accounting Office and Front Office had business-hours access to the Bryant Space Sciences Research Building machine room (central computer room) via its issued access cards. Further, the core network rooms located throughout the University campus were secured under the University's master key system. As a result, keys could be issued to multiple parties without measures in place for CNS management to authorize, account for, or monitor the issuance and use of these keys. In response to our audit inquiries, CNS staff indicated that the University has a plan to re-key the locks and that CNS is researching the possibility of not using the University lock system. The absence of adequate controls in place to physically secure IT facilities and resources exposes the University to risk of loss through unauthorized access, misuse, or resulting damage to equipment.

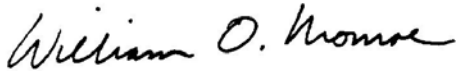
Recommendation: The University should review granted access for appropriateness and proceed with efforts in establishing a more secure access system to authorize and adequately monitor access to the remote network rooms.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected University IT controls, including management's control framework for securing the application and the surrounding technology infrastructure. Our scope focused on evaluating selected internal controls and IT functions applicable to PeopleSoft Financials during the period July 2005 through December 2005. 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, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated March 15, 2006, the University provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

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.

APPENDIX A
MANAGEMENT RESPONSE



Finance and Administration
Office of the Vice President

204 Tigert Hall
PO Box 113100
Gainesville, FL 32611-3100
(352) 392-1336
Fax (352) 392-6278

March 15, 2006

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

Dear Mr. Monroe:

Enclosed is our response to the preliminary and tentative findings and recommendations for the Information Technology Audit of the University of Florida PeopleSoft Financials System, administered by the State of Florida for the period July 2005 through December 2005. We will implement the recommendations identified during the audit in accordance with the enclosed schedule of responses.

Thank you for your continuing support of the University of Florida. Please contact me if I can provide additional assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "Ed Poppell".

Ed Poppell, Vice President
for Finance and Administration

Enclosures

- cc: Dr. J. Bernard Machen, President
- Mr. Robert Miller, Associate Vice President for Finance and Administration
- Ms. Nur Erenguc, Inspector General
- Mr. Michael V. McKee, University Controller
- Mr. Michael Corwin, IT Principal - Bridges
- Mr. Mark Hoyt, Interim Assoc. Provost for IT & Professor
- Board Members

An Equal Opportunity Institution

**UNIVERSITY OF FLORIDA
RESPONSES TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS
FLORIDA PEOPLESOFT FINANCIALS SYSTEM
FOR THE PERIOD – JULY 2005 THROUGH DECEMBER 2005**

Background

The University commenced a multi-year project, commonly referred to as Enterprise Resource Planning (ERP), in Fall 2002 to replace the University's legacy systems (FLAIR) with new web-based systems that would provide real-time information and to respond to the reorganization of Higher Education. In February 2003, this project was named the *UF Bridges* project.

To save on licenses, maintenance, and implementation costs, the University formed a consortium with Florida State University and Florida Agricultural and Mechanical University. The University of Florida purchased software applications for finance, including general ledger, purchasing, accounts payable, expense/travel, asset management, sponsored programs and accounts receivable, and for human resource, including payroll and benefits. Additionally, software applications were acquired for portal (web access) and enterprise reporting. All of these new integrated applications are collectively called the *myUFL systems*. With a "go-live" date of June 18, 2004, the new applications were used for University business processes effective July 1, 2004.

The University established a "go-live" date of June 18, 2004, with the advice and counsel of the State Comptroller's office since the state's financial system was to change at about the same time (2004) and UF did not wish to experience two conversions. With this direction UF had only eighteen months to implement a Payroll, Human Resource and Financial system. This very aggressive and compressed time frame did not allow for extended planning and training. The University of Florida believes this background is critical for proper reflection on the observations cited by this audit.

Item 1a - University had not conducted a risk assessment specific to myUFL systems.

University Response - UF Bridges will conduct a risk assessment project to produce formal documentation of risks associated with the operation of the myUFL systems. This project will include input from core business areas and will address the following; architectural framework of myUFL, user authentication, and role authorization aspects of myUFL systems. The report will be provided to the University ISM and reviewed annually to comply with current university IT Security and Risk Assessment policy. The review will be lead by the Bridges Level 2 ISM, and will be completed by May 1, 2006.

Item 1b – University lacked written standards for authorized transmission of the myUFL system data over emerging technologies.

University Response - All traffic to and from the myUFL systems is encrypted using the most secure commercially available technology. The University does not believe additional written standards are needed regarding transmission of my UF data.

Item 1c – University lacked defined procedures for complying with its IT Data Security Standard's policy regarding annual review of employee access.

University Response - The Bridges Level 2 ISM has begun a project to formalize the certification process within the Access Request Security (ARS) application. Departmental Security Administrators (DSA) will be required to review security of all individuals in their control area at least once each 365 day period. For non-UF employees certification must take place every 180 days. Notices will be sent in advance of the certification deadline to a DSA indicating a review is necessary. Procedures will be documented and added to the DSA training program on WebCT, and written procedures will be available on the Bridges Website. Once developed this process and monitoring solution will provide a tool to drive compliance of the annual review requirement. The estimated completion date is April 30, 2006.

Item 1d – Written procedures were not in place to ensure the removal of user roles of the deletion of user sign-on accounts.

University Response - The cleanup of myUFL security data has been underway since November 2005. New monitoring software to track changes to staff and non-employee relationships was put into production on Feb. 25, 2006. Department DSA's and Bridges security team are notified daily of personnel actions which require DSA review of user role authorizations. DSA's are asked to respond to the Bridges Security team regarding the action they have taken or the reason why no action is required. A response is required from the DSA in all cases. The Bridges Security team will ensure that responses and action(s) taken for each notification are retained and tracked for appropriate compliance to UF policies. Procedures for these reports and notifications will be documented in procedures and forwarded to the UF ISM for review. Record retention and documentation of any actions taken by the Bridges Security team will be maintained in files at UF Bridges. Complete documentation with instructions to DSA will be completed by April 30, 2006.

Item 1e – Provisions for recovery of the myUFL systems, along with measures and schedules to test recovery procedures, had not been formally documented.

University Response - The Bridges Disaster Recovery document will be enhanced and updated to include myUFL systems. Current recovery plans are in place for all legacy systems that include all University Financial operations, UF Directory Operation and

other applications which operate under the control of UF Bridges. An interim plan will be created for the critical functions in conjunction with the Risk Assessment. This interim plan will be complete by December 1, 2006.

Item 1f – Training for the PeopleSoft applications was not mandated by the University and did not include security awareness training for handling data and preserving its confidentiality.

University Response - The University does not mandate training for all PeopleSoft applications; however all DSA's are required to attend training, as are all users of the new electronic Personnel Action Form (ePAF). At this time there is no plan to further mandate training for all PeopleSoft applications. Expanded and exhaustive training for application functionality has been underway since go-live and has provided continually improved end user processing. Bridges staff will work with the University ISM to publish training material regarding downloading and securing of data from the myUFL system. Completion: July 31, 2006.

Item 1g – University's IT Data Security Standard listed disposal methods a step under Data Classification Guidelines..... However, the standard did not detail specific procedures....

University Response - This observation has been corrected. The data standards now link to existing university surplus property processes that provide procedures for data cleansing. The University will review current contractual provisions with contractors (including consultants) regarding confidential information and determine the appropriate method to ensure that contractors properly dispose of all confidential University information. Completion date: June 30, 2006.

Item 1h – UF Bridges staff had not undergone background checks or signed confidentiality agreements

University Response - Entrance procedures for all Bridges staff have been updated to include the signature on confidentiality agreements which provide acknowledgement of duties related to their positions of special trust and confidentiality responsibilities. All current and future Bridges staff will be made aware of the IT Policies and documents which we are obliged to observe and staff will be provided with a procedures document for Change Control and Security procedures at UF Bridges by April 15, 2006. UF Bridges policy requires all staff and consultants hired since August 2005 to have background checks performed.

Item 1i – Written change control procedures for myUFL did not include procedures to ensure changes or customizations are ADA compliant

University Response - PeopleSoft Applications are delivered with ADA compliant features. The university also has policy for Web page accessibility and a Disabled Access Computing Policy. Bridges has identified that during the Change Management

Peer Review Process system modifications will be reviewed for compliance with PeopleSoft ADA and /or University ADA guidelines depending on the origin or environment that the software operates within. All Bridges development staff will be provided ADA compliance procedures and those staff responsible for peer review oversight will be provided in service training to assure they understand the nature of the requirement of this compliance related issue. It will be the responsibility of peer reviewers to indicate and check off that ADA considerations have been reviewed. Specific written procedures will be developed and incorporated in the change control and development procedure documentation. Completion Date: March 17, 2006.

Item 1j – University had not formally defined circumstances or designated personnel for correction usage

University Response - UF Bridges Security team and functional areas will work with each core user area to define appropriate procedure and policy for use of correction mode. Members of UF Bridges and core user areas will form a project to conduct a complete review of this topic and make specific policy and procedure recommendations to Bridges management. Subsequent to those recommendations, a project team to improve the issues with correction mode usage will be formed to achieve compliance with the recommendations on policy and procedure. The policy recommendation portion of this work will be completed by May 1, 2006. Implementation of the policy and procedures will be completed by December 1, 2006.

Item 1k – University did not require the University's business unit local networks to join under Active Directory

University Response - The University offers 3 options to application systems for secure authentication. It is a management decision as to which of the three systems are used.

Item 2a – Bridges personnel maintained access to perform financial transactions

University Response - It is necessary that Bridges personnel have access to perform financial transactions. As part of on-going day to day operations during implementation and stabilization, Bridges is responsible for supporting the functional areas in monitoring and correction of certain financial transactions. Bridges only updates financial transactions in the event of production critical situations. As stabilization occurs, Bridges and core offices continue to evaluate and remove access as they establish roles and responsibilities.

Item 2b – Two Bridges staff members not part of the security team had access to update security

University Response - A report will be provided to the Bridges ISM on a weekly basis to review access roles for managing security. Beginning April 1, 2006 Bridges Level 2 ISM will review, initial and file these sensitive role assignments. All inappropriate access to

update myUFL security has been removed. Only members of the myUFL security team have access to update any portions of myUFL security.

Item 3 – Control deficiencies were noted in myUFL systems environment related to system logging, password and user workstation controls, network authentication, wireless access, and operations system controls.

University Response - Corrective action will be taken to respond to the confidential findings. To address the control deficiencies, written procedures and policies will be in place on July 1, 2006.

Item 4 - Absence of adequate controls over physical security and access necessary to protect IT facilities and resources.

University Response - The CNS central computer room in the SSRB building is staffed 7X24. To enter the room you must pass through 2 locked security doors. Each door requires card key access. Whenever a card key is used to open a door, an entry is logged to record the event. The log entry identifies the card-key owner, the date, the time, and the door. We will review all current card keys issued for appropriateness and we will remove computer room access from CNS staff who do not have job duties that require it.

THIS PAGE INTENTIONALLY LEFT BLANK