FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

AUDIT OF THE INFORMATION TECHNOLOGY CONTROLS OVER THE PEOPLESOFT GRANTS MODULE

Report No. 10/11-08

February 8, 2011

FIU | FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: February 8, 2011

To: Robert Grillo, Interim Vice President of Information Technology & CIO
Andres Gil, Vice President for Sponsored Research

From: Allen Vann, Audit Director

Subject: **Audit of the Information Technology Controls Over the PeopleSoft Grants Module - Report No. 10/11-08**

We have completed an audit of the Information Technology Controls Over the PeopleSoft Grants Module. The Grants Module, which was put into production in June 2009, accumulates cost and budgeting data which facilitates billing and financial management of each approved award. The total amount awarded to Florida International University researchers for the year ended December 31, 2010 was $104,330,662.

Our audit concentrated in four control areas: 1) User Account management, 2) Identity management, 3) Segregation of Duties, and 4) Workstation security. We found security deficiencies related to the temporary user account management process. The identity management process also needed improvement. We also found privileged users were allowed to update their own profiles, which violates key segregation of duties precepts. In addition, management had key navigation access not typical or necessary for their positions. Finally, workstation security's monitoring capabilities were not operating properly. The audit resulted in 34 recommendations. Management agreed to implement all of our recommendations.

We wish to express our appreciation for the cooperation and courtesies extended to us by UTS, IT Security Office, OSRA, and the Controller's Office while conducting the audit.

C: Albert Maury, Chair, and Members of the Finance and Audit Committee
Mark Rosenberg, University President
Douglas Wartzok, Provost & Executive Vice President
Kenneth Jessell, Chief Financial Officer & Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President
Joseph Barabino, Associate Vice President for Research
Tonja Moore, Associate Vice President Academic Affairs, Provost Office
Cheryl Granto, IT Security Officer

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Our audit focused on the Information Technology processes relating to user activation, identity management, segregation of duties for privileged user accounts, and workstation security as it may affect or is directly related to the Grants Module.

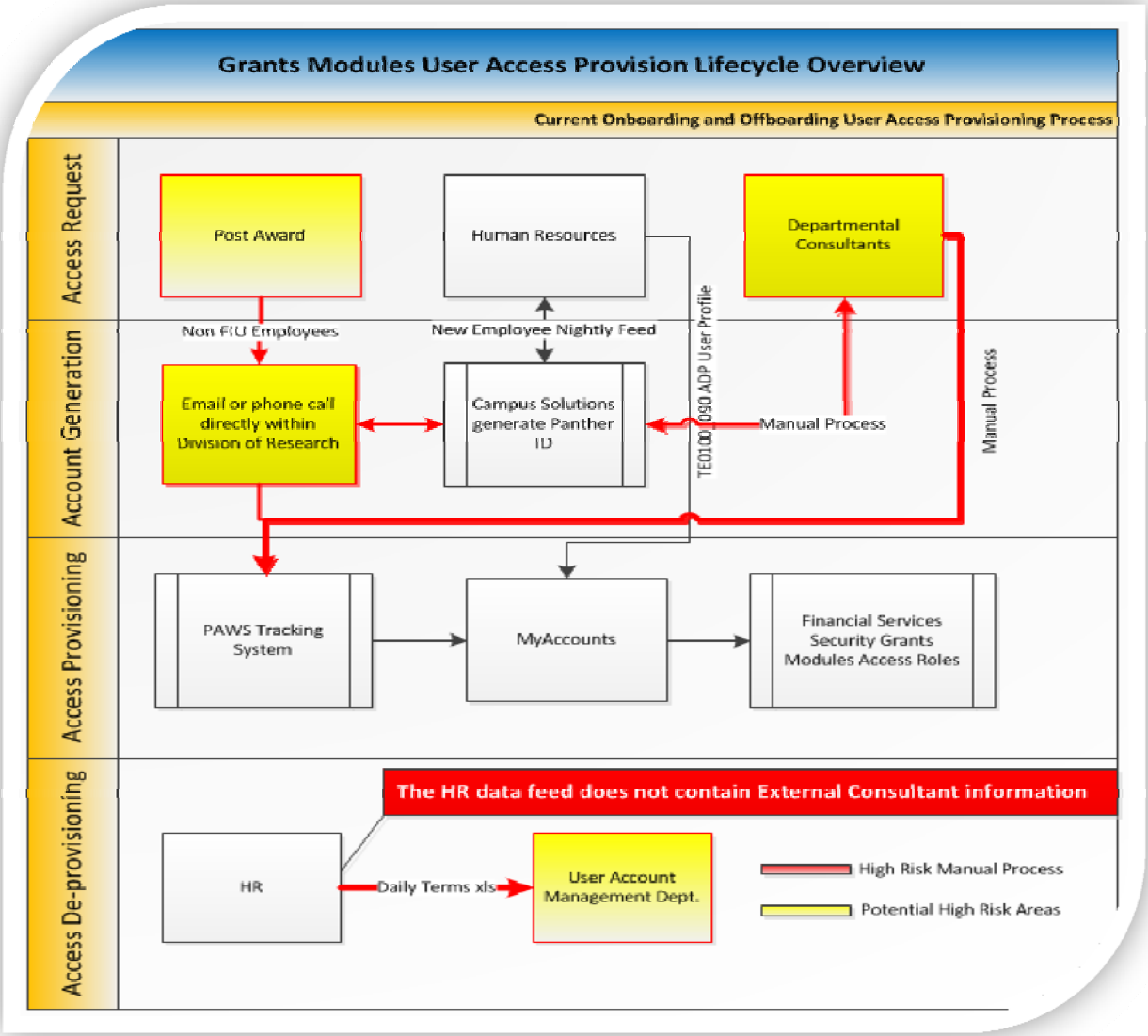


Figure 1

We concluded that the on-boarding "user account activation" and off-boarding "user account deactivation" process of accounts (see Figure 1) have security deficiencies for non-FIU and Consultant accounts. Staff efforts focused on expediting the on-boarding process for consultants and non-FIU temporary employees through a manual process consisting of generating Panther IDs through Campus Solutions and then manually entering their access onto the Grants Module. Bypassing the current automated process

and neglecting to perform periodic user account reviews resulted in an unnecessary risk security gap in user account management.

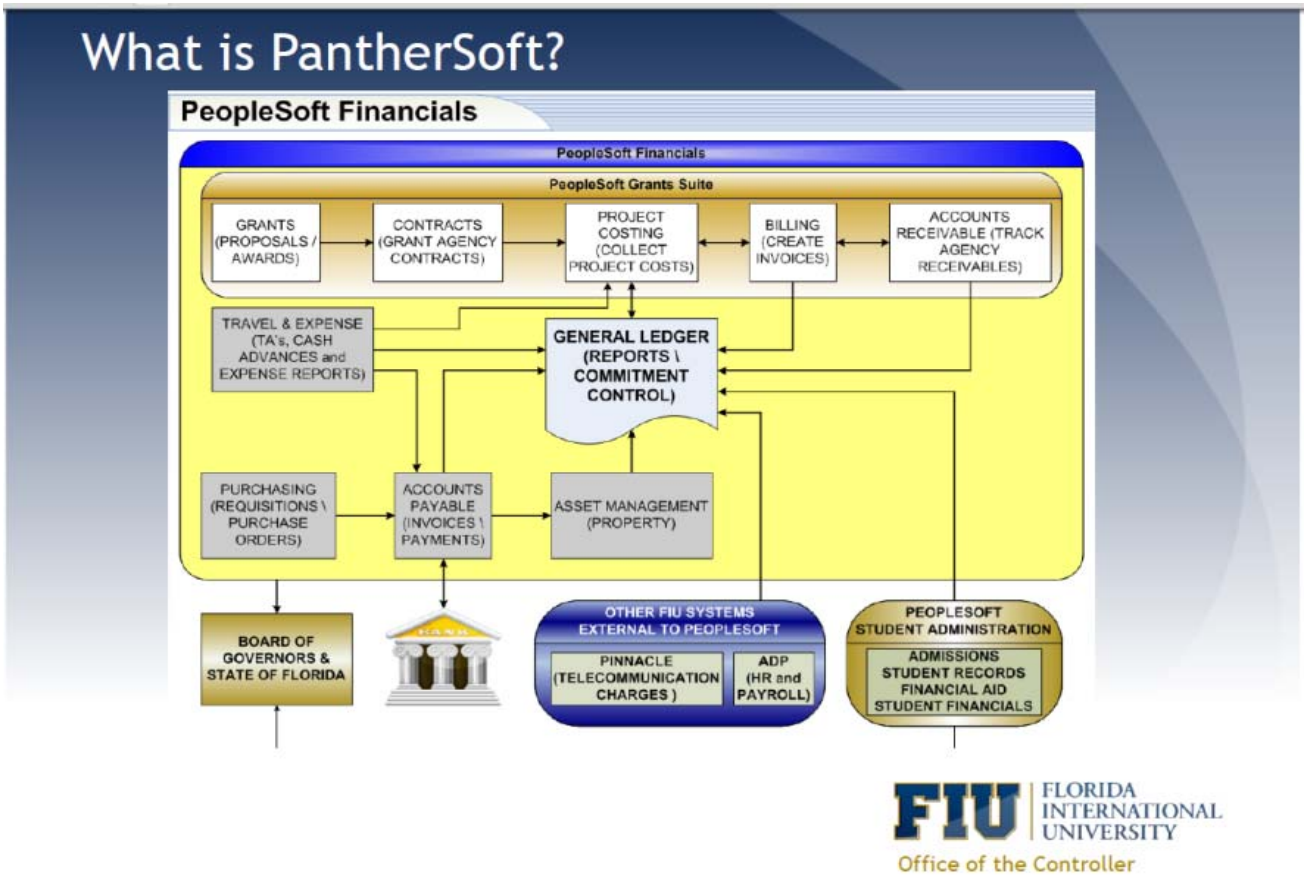
Good internal controls are implicitly stated through the use of roles and permissions. However, terminated users still had active permissions on key roles. We found that three consultants, with Billing and Account Receivable Super User access, remained active 60 days after their contract expired. In addition, the consultant accounts still had active accounts including, Active Directory, Employee Self-Service, and VPN access. The user security deficiency is primarily due to the manual notification process currently in place which is outside of the automated employee process from the Human Resources Department. Consultants and non-FIU temporary Grants Module access remains active unless the PantherSoft – Financial Systems Department is notified. User account management efforts should focus on automating the off-boarding of consultants and non-FIU temporary employees. While Identity Management processes include established roles and permission lists, the process of requesting access for temporary and non-FIU users is informal. In our Least Privilege account access testing, we found upper level management with access not typical of their job duties.

Most of the Security Administrators tested (four out of seven) had updated their own profiles with no required review or approval. We also discovered that both staff and upper level management have Security Administrator access. Typically upper level management reviews and approves access requests and therefore should not also have the ability to create, modify, or delete user access as this creates a segregation of duties control risk. The PantherSoft Security policies reviewed were not adequately maintained. Good procedures start with compliant policies. Security procedures should be reviewed by the IT Security Office and Compliance Department prior to production release.

Workstation security is a universally accepted necessity. We found during our testing, however, that there is no monitoring to verify whether malicious code protection mechanisms are working properly. In addition, the anti-virus monitoring mechanism was disabled on the workstation of one of the grant's module administrators.

BACKGROUND

The Grants Module (or Module) was placed into production in June 2009. The Module replaced the previous process of storing post award grants information on spreadsheets. The Module includes: 1) Grants Management; 2) Project Costing; 3) Contracts; 4) Billing; and 5) Accounts Receivable.



1. ***Grants Management*** stores "demographic" information relating to sponsors, professionals, sub-recipients, and FIU departments. Presently, the Pre-award (proposal entry and proposal budget) process is handled by a separate application: *Info Ed*. Information regarding grants, such as the approved budget, is entered into this Module after grants are awarded. Additionally, the F&A (Facilities and Administrative) configuration and calculation data is also entered into the Module.

2. ***Project Costing*** collects expense data from other modules (i.e., Accounts Payable, General Ledger, Travel and Expense) for billing purposes. The Project Ledger contains detailed transaction data for all sponsored program activities, including budgets, expenses, and billings.

3. ***Contracts*** contain the detail setup information required for each approved award to facilitate billing, revenue recognition, and amendment processing.

4. ***Billing*** processes billing information to create invoices. The billing module allows the ability to standardize and optimize billing activities whereby all invoices are appropriately reviewed and validated.

5. ***Accounts Receivables*** enables the Office of Sponsored Research Administration (OSRA) to enter and track grant receivables, receive and apply payments, and manage outstanding receivables.

The PantherSoft–Financial System Department, part of the PantherSoft and Administrative Software Unit, is responsible for the Module's security.

OBJECTIVES, SCOPE, AND METHODOLOGIES

As part of the approved work plan for the fiscal year 2010-2011, we conducted an audit of the Information Technology Controls Over the PeopleSoft Grants Module for the period July 1, 2010 through November 30, 2010. Audit fieldwork was conducted from October 18 to November 23, 2010. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

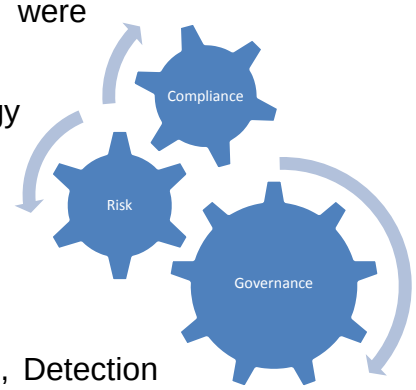
As part of our audit, we reviewed internal and external audit reports issued during the last four years to determine whether there were any prior recommendations related to the scope and objectives of this audit and whether management had effectively addressed prior audit concerns.

We found that in the Auditor General Report No. 2007-006, dated July 2006, deficiencies were noted in the University's procedures for restricting access to appropriate users and application environment and support function. Auditor General Report No. 2007-006 Findings No. 2 and No. 3 are noted, where applicable, in Appendix A - Control Objectives as detective controls[1].

The scope of the work performed focused on the evaluation of software access controls and internal user account management controls associated with the Grants Module. The objectives of this audit included:

- The adequacy of the current process regarding the addition, modification, and removal of user access within the Grants Module.
- The appropriateness of current user access specific to privileged and other high risk access within the Grants Module.
- The adequacy of Segregation of Duties specific to privileged user accounts within the Grants Module.
- Determining that basic security measures have been implemented for end user workstations within the Grants Module. (The IT Security Office assisted us in performing workstation testing.)

To achieve these objectives, the following methodologies were applied:



- Control Objectives for Information and related Technology (COBIT) 4.1 (See COBIT Methodology on page 9).
  - o Deliver and Support 5.4 User Account Management
  - o Deliver and Support 5.3 Identity Management
  - o Plan and Organize 4.11 Segregation of Duties
  - o Plan and Organize 4.12 IT Staffing
  - o Plan and Organize 4.13 Key IT Personnel
  - o Deliver and Support 5.9 Malicious Software Prevention, Detection and Correction

[1] A detective control is designed to find an error after it has occurred so that the error can be corrected.

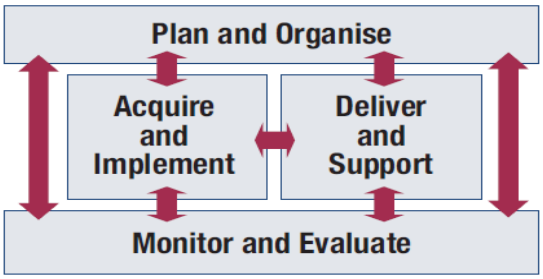
- National Institute of Standards and Technology Special Publication (NIST) 800-53A Revision 1
  - Access Control Policy and Procedures 1.1
  - Account Management 2.1
  - Account Management 2(1), 2(2), 2(3)
  - Personnel Termination 4.1

Staff interviews provided us with an overall understanding of the PeopleSoft Grants Module, security policies and procedures, and user access lifecycle process flows related to user account management. Selected individuals were queried about their various roles, responsibilities and the process in which they receive information pertinent to the establishment, modification, and removal of Grants Module User Access. From these interviews, additional testing including: on-site inspections and visual and hands-on observations were conducted in order to identify high risk vulnerabilities and potential gaps in security.

Data reliability, COBIT Deliver and Support 11.6, was not tested and therefore not covered in this report. Data reliability will be tested and covered in subsequent grant related audits.

The COBIT Methodology

The Control Objectives for Information and related Technology (COBIT) is a set of internationally recognized information technology (IT) best practices in a framework focused on the alignment of IT and the business units it supports. COBIT provides "what" IT controls to be implemented. The COBIT 4.1 framework has 34 high-level processes, covering 210 control objectives, which are categorized in the following four domains:



- Plan and Organize (PO)
- Acquire and Implement (AI)
- Deliver and Support (DS)
- Monitor and Evaluation (ME)

COBIT is a comprehensive framework. The COBIT framework provides control objectives specific to the area of concern, with a centralized viewpoint, from which senior management provides direction; management aligns their processes; and internal audit reviews its controls.

COBIT's maturity modeling over IT processes is based on a method of evaluating existing processes in a measurable fashion. A maturity model has been defined for each of the 34 COBIT IT processes, providing an incremental measurement scale from:

0-Non-existent: Management processes are not applied at all
1-Initial | Ad Hoc: Processes are ad hoc and disorganized.
2-Repeatable but Intuitive: Processes follow a regular pattern.
3-Defined Process: Processes are documented and communicated.
4-Managed and Measurable: Processes are monitored and measured.
5-Optimized: Good practices are followed and automated.

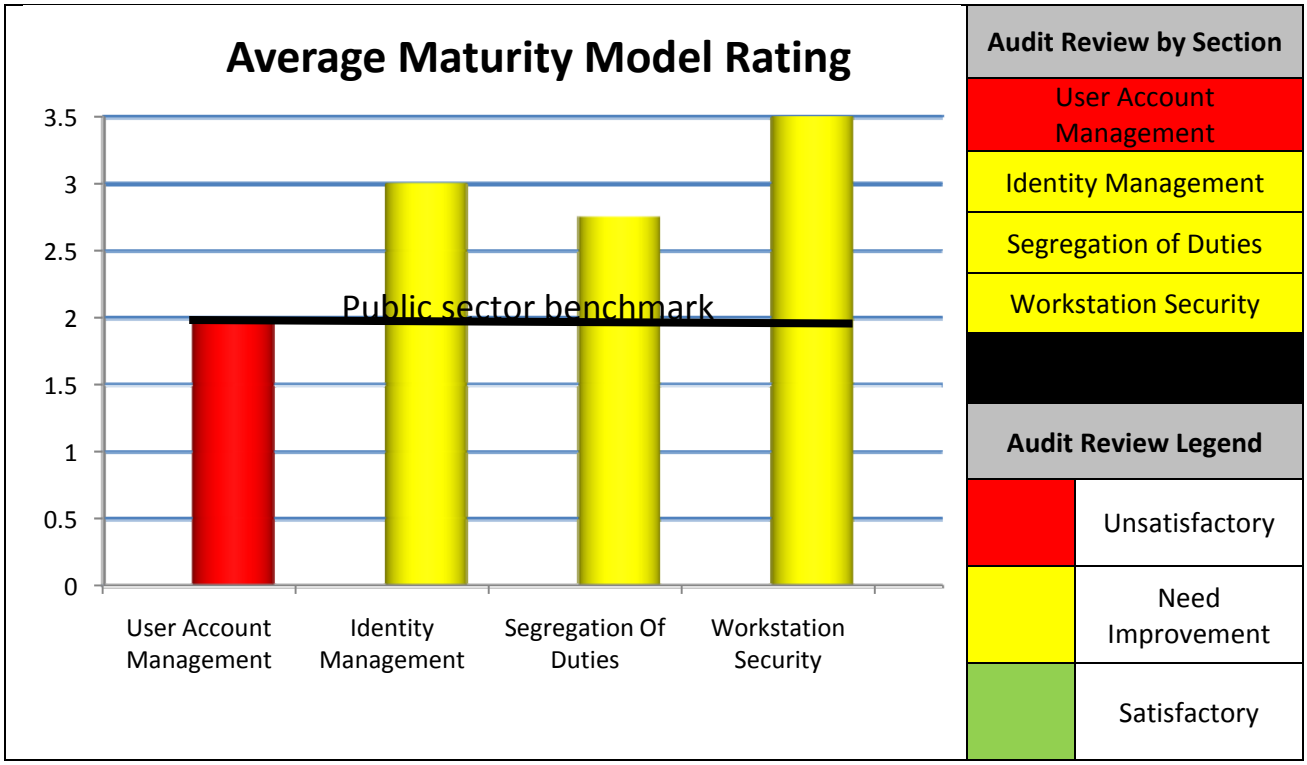
Using the maturity models developed for each IT process, management can identify:

- The actual performance of the process in relation to where it is today.
- How the process benchmarks to others in the public sector industry[2].
- Management's target for process improvement in order to obtain where it wants to be.

The purpose of maturity modeling is to identify where issues are and how to set priorities for improvements. With COBIT maturity models, there is no intention to measure levels precisely or try to certify that a level has exactly been met.

[2] Benchmark results are provided by Information Systems Audit and Control Association (ISACA) COBIT Online, based on the public sector industry; with a staff greater than 1500; located in North America.

AUDIT DASHBOARD



The chart listed above displays the average maturity model rating for each COBIT Control Objective tested. COBIT Deliver and Support 5 control objectives reviewed in this audit are represented by User Account Management (DS5.4), Identity Management (DS5.3), and Workstation Security (DS5.9), respectively. COBIT Plan and Organize 4 control objectives reviewed in this audit are represented by Segregation of Duties (PO4.11).

The Audit Review section, in relation to the above COBIT control objectives tested, highlight whether the controls perform:

- **Unsatisfactory** - Potentially serious security gap in policy and or procedure which may adversely affect the confidentiality, integrity and availability of system data.

- **Need improvement** - A potential security gap in policy and or procedure which may adversely affect the confidentiality, integrity and availability of system data.

- **Satisfactory** - No security gaps in policy and or procedures were noted.

FINDINGS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

Findings	Recommendations	Management Responses
A. User Account Management		
A.1 (see page 22)		Maturity Model: 3
There is a formal security policy and security role handbook, which details access procedures. The security role handbook is periodically updated; however, there is no defined frequency for policy reviews. We also noted that the security policies are not reviewed by the Compliance Department prior to release.	1a) Security policies should be reviewed on a defined frequency. 1b) Security policies should be reviewed by Compliance Department prior to release.	1a) Financial Security *Policy* was renamed to Financial Security *Procedure.* Information Technology Security Office (ITSO) was given access to the PantherSoft SharePoint site and the procedure will be reviewed by ITSO whenever changes are made. Grants security handbook is being updated regularly to reflect any updates to Grants security. We implemented a procedure where any changes to this handbook will be tracked via SharePoint version control functionality with appropriate comments. **Implementation Date**: Immediately 1b) The Financial Security Procedure will be submitted to the University Compliance Officer by February 15, 2011 for review and feedback purposes. **Implementation Date**: Immediately

Findings	Recommendations	Management Responses
A.2 (see page 23)		Maturity Model: 2
In response to Auditor General Finding No. 3, the Grants Module user access procedure combines an automated and manual process. There is an established procedure which integrates an automated onboarding and offboarding procedure for FIU employees. Non-FIU user accounts are onboarded and offboarded through a manual process. There is an informal notification process for non-FIU user accounts. Exceptions were found for three consultants whose Grants Module access was active up to 60 days after their contract expired. We noted that user accounts are not periodically reviewed by department managers. Consultant accounts were not adequately removed in a timely fashion. In addition, consultant accounts were still active in MyAccounts. We also noted that the offboarding process for consultant and non-FIU employees was not included in the security policy.	2a) Non-employee accounts, such as Consultants, should be incorporated into the established automated onboarding and offboarding processes. 2b) Consultant and temporary accounts should be onboarded with expiration dates to automatically begin the offboarding process unless approved by management as their contract and or job duties dictate. 2c) User accounts should be periodically reviewed by department managers to ensure user access is appropriate and used as intended. 2d) Offboarding process for consultants and non-FIU employees should be included in the security policy.	2a) Human Capital Management (HCM) project that is in the process of being implemented includes functionality that allows automating of the onboarding and offboarding processes for non-employee constituents. We will leverage this functionality to remedy this finding. **Implementation Date**: January 1, 2012 2b) The functionality referred in 2a) will include begin and end dates according to non-employee contracts or statements of work. **Implementation Date**: January 1, 2012 2c) The Division of Research will continue to review user access. Going forward on a quarterly basis, based on the HR report listing employees that changed departments, Research Decision Support will provide the Division of Research Directors a report of PeopleSoft Grants Functional Roles assigned for review and confirmation. **Implementation Date**: Immediately 2d) Financial Security procedure will be updated upon deployment of the HCM functionality outlined in 2a). **Implementation Date**: January 1, 2012

Findings	Recommendations	Management Responses
	2e) Consultant accounts should be removed from all information systems.	2e) The Human Capital Management project function mentioned in 2a). **Implementation Date**: January 1, 2012
A.3 (see page 23)		Maturity Model: 2
There is no automated process for terminating consultant or non-FIU temporary access accounts. There are no time limits on consultant or non-FIU temporary accounts. Consultant or non-FIU temporary accounts must be manually removed through the Financial System Services Group and the User Management Group. Presently, there is no unified communication between the two groups. ADP termination feeds use the TETIDAL batch account on a nightly basis.	3a) Temporary accounts, including consultants and non-FIU users, should include start and end dates which corresponds to either their contract or project. An automated trigger mechanism should automatically start the offboarding process unless documented approval from appropriate management. 3b) All inactive Grants Module accounts should be automatically disabled after a defined period of time.	3a) The Human Capital Management project function mentioned in 2a). **Implementation Date**: January 1, 2012 3b) The Human Capital Management project function mentioned in 2a). **Implementation Date**: January 1, 2012
A.4 (see page 24)		Maturity Model: 2
The PeopleSoft application, a superset of the Grants Module, tracks who last modified user profile and date modified, last date that password changed, and last date user logged in. System Administrators are not notified when profile access levels have changed.	4a) In addition to the existing tracking capabilities, the user account audit trail should include role modified date, account creation date, and account disable date.	4a) To leverage delivered PeopleSoft functionality we will deploy the Field Audit where all dates associated with the user account will be tracked. **Implementation Date**: April 30, 2011

Findings	Recommendations	Management Responses
	4b) An automated trigger mechanism should notify the system administrators group when privileged and or sensitive access has been granted.	4b) PeopleSoft Financial Security does not differentiate between privileged and regular accounts. Since security changes to all user accounts are recorded and tracked via PAWS system, the Security Administrator, Customer (user) and Requestor are being notified through the PAWS notification system. **Implementation Date**: Immediately
A.5 (see page 25)		Maturity Model: 2
Privileges accounts are based on role access schemes FIU_Security_Admin" and "FIU_Security_Admin_LTD01", respectively. In response to Auditor General Finding No. 3, privileged role assignments are tracked in the PAWS application. However, we noted that Privileged user access roles are still not monitored, documented or retained.	5a) Privileged user accounts should be monitored for accuracy and relevance to current job position. 5b) Privileged user access reviews should be performed by management and formally documented and retained.	5a) These specific privileged accounts are documented in the Financial Security procedure and Distributed User Profile documents. Their assignment is approved by the PantherSoft Assistant Director and recorded in the PAWS change management system. The PantherSoft Assistant Director reviews these specific roles on a semi-annual basis. **Implementation Date**: Immediately 5b) Refer to response in 5a). **Implementation Date**: Immediately

Findings	Recommendations	Management Responses
B. Identity Management		
B.1 (see page 26)		Maturity Model: 3
All user accounts are grouped by role type (i.e., FIU_BI_Specialist). In response to Auditor General Finding No. 3, group membership is defined in the PantherSoft Financials Security Policy. Access requests are documented in the PAWS tracking application. We noted, however, consultants and non-FIU access process is still informal. We noted that temporary user accounts consultants and non-FIU temporary users, are not monitored.	6a) Departments Managers who are requesting approved consultants and non-FIU temporary users should enter the request directly into PAWS thereby documenting the user's access level approval. 6b) Ensure that user access rights are requested by department management, approved by system owners and implemented by the IT security personnel. 6c) Usage of temporary user accounts, including consultants and non-FIU employees, should be monitored.	6a) FIU leverages existing support structure of PeopleSoft Financials, including Grants. Research Decision Support (RDS) group was established as a liaison between the Division of Research central staff and PantherSoft. While the Division of Research department managers do not have access to PAWS, they can initiate a security request for their employees through the Division of Research SharePoint site. Based on that documented request, RDS will enter PAWS security request that will be implemented by Security Administrator. All Grants security roles had been reviewed and pre-approved by Associate V.P. Research Programs. **Implementation Date**: Immediately 6b) Refer to response in 6a). **Implementation Date**: Immediately 6c) Refer to response in 6a). **Implementation Date**: Immediately

Findings	Recommendations	Management Responses
B.2 (see page 26)		Maturity Model: 3
The University indicated that extraneous user access was granted during implementation to aid in application processes and debugging. We noted that the Grants Module permission lists do provide the ability for finer-grained user privileges. In response to Auditor General Finding No.3, super user account FIU_ Security_ Admin is limited to three Administrator Software coordinators and Assistant Director. In response to Auditor General Finding No. 3, FIU_Security_Admin_LTD01 is limited to three Deputy Controller accounts (Associate Controller, Business Analyst, Sr. Computer Support) and the Assistant Director – University Computer Systems.	7a) As the implementation of the Grants Module has been completed, least privileged access to super user accounts should be allowed only to accomplish assigned tasks and business functions. 7b) Assistant Director of University Computer Systems is in an overview position and should therefore be removed from the access privileges FIU_Security_Admin and FIU_Security_Admin_LTD01, respectively. 7c) Associate Controller is in an overview position and should therefore be removed from the FIU_Security_Admin_LTD01 access privileges. .	7a) Management agrees that during the post-implementation phase of the Grants Module, user's access privilege will be evaluated and appropriately paired down to take into account individual roles and responsibilities, while preserving efficient production support and maintaining effective internal controls. **Implementation Date**: Immediately 7b) FIU_SECURITY_ADMIN was assigned temporarily to the Assistant Director of University Computer Systems as a backup. FIU_SECURITY_ADMIN is no longer assigned to the Assistant Director. **Implementation Date**: Immediately 7c) FIU_SECURITY_ADMIN_LTD01 was created to support delivered Distributed User Profile functionality where certain group of users sharing the same security is allowed to assign Inquiry Only roles to the rest of the organization. This applies to Financial System Support group where members of this group were granted this role, including the Associate Controller. At this moment FIU_SECURITY_ADMIN_LTD01 role is no longer assigned to the Associate Controller. **Implementation Date**: Immediately

Findings	Recommendations	Management Responses
C. Segregation of Duties		
C.1 (see page 27)		Maturity Model: 3
In response to Auditor General Finding No. 3, there appeared to be adequate segregation of duties between Security Admin access and FIU_BI_Specialist, FIU_AR_Specialist, or FIU_BI_AR_Manager access. Users did not have incompatible roles. However, 4 out of 7 Security Administrators tested personally updated their profiles through their own account.	8) Privileged users should not be allowed to update their own profiles.	8) There are few people who have privileged role of FIU_SECURITY_ADMIN. The Financial Security Procedure was updated to reflect this stipulation and this access will be monitored by the FS PantherSoft Manager via Query. **Implementation Date**: Immediately
C.2 (see page 27)		Maturity Model: 3
Roles and permissions are outlined in job duties and serve to adequately document segregation of duties. FIU_Security_Admin and FIU_Security_Admin_LTD01 access levels are not listed in the Security Policy or Security Role Handbook.	9) FIU_Security_Admin and FIU_Security_Admin_LTD01 should be listed in the Security Policy and or the Security Role Handbook.	9) 'Financial Security Access' and 'PantherSoft – Distributed User profiles' documents describe both roles in details. **Implementation Date**: Immediately
C.3 (see page 28)		Maturity Model: 2
In response to Auditor General Finding No. 3, we selected FIU_BI_AR_Manager, FIU_AR_Specialist, and FIU_BI_Specialist to represent sensitive access roles in Billing and Accounts Receivables. In examining those roles we found: FIU_BI_AR_Manager: 1 terminated employee. 3 terminated consultants. 1 Director Research Programs.	For the FIU_BI_AR_Manger role: 10a) Terminated employees and consultants should be removed. For FIU_AR_Specialist role: 10b) Terminated consultants and Upper-level management (Associate V.P. and Director) should be removed.	10a) All terminated employees and consultants have been removed for the FIU_BI_AR_Manger role. **Implementation Date**: Immediately 10b) Consultants that have been terminated have been removed and for Upper level management, refer to 7a). **Implementation Date**: Immediately

Findings	Recommendations	Management Responses
FIU_AR_Specialist: 3 terminated consultants. 1 Associate V.P. Research Programs.* 1 Director Research Programs. 3 Coordinator Research Programs. FIU_BI_Specialist: 1 Director Research Programs.* 1 Coordinator Research Programs. 3 Grants Specialist. *Based on their job function, it is not typical for Upper level management to have or need access.	For FIU_BI_Specialist role: 10c) Access for Upper-level management (Director Research Programs) should be removed.	10c) Refer to response in 7a). **Implementation Date**: Immediately

Findings	Recommendations	Management Responses
D. Workstation Security		
D.1 (see page 28)		Maturity Model: 3
In response to Auditor General Finding No. 2, workstations are protected by McAfee On-line Access Scan (OAS) feature. The OAS automatically checks files prior to opening, including email attachments and removable media files. We found the OAS feature on workstation ADS9D43 was disabled, which increased the risks exposure of the workstation to malicious software and related viruses. The OAS logs ended on 08/11/2010, indicating that workstation ADS9D43 may have been susceptible to viruses from 08/11/2010 to present. The system event logs further revealed an error message repeated from 08/11/2010 to 11/23/2010: "The McAfee McShield service depends on the following nonexistent service: mfevtp". This indicates that OAS version 8.7i was inappropriately removed. The potential security risk of OAS being disabled when accessed by a privileged user as in the case of workstation ADS9D43 is used by a privileged user on the System Security Team within the Grants Module.	For privileged and sensitive workstations: 11a) McAfee OAS feature should be enabled on workstation ADS9D43. In addition, workstation ADS9D43 should be checked for malicious software which may be residing due to the OAS being disabled. 11b) Reporting mechanisms should be established to ensure malicious software applications are properly functioning on all workstations. 11c) Workstation event logs should be periodically reviewed to ensure malicious software applications are properly functioning.	11a) OAS will be enabled and the computer has been checked for malicious software. **Implementation Date**: Immediately 11b) We currently have McAfee EPO to serve this function. An investigation is underway to determine the cause for the gap in coverage. **Implementation Date**: April 30, 2011 11c) EPO can be configured to send alerts on behaviors indicating the presence of malicious software. This feature needs to be tested prior to implementation. **Implementation Date**: April 30, 2011

Findings	Recommendations	Management Responses
D.2 (see page 28)		Maturity Model: 4
Virus signature definitions are continuously updated by McAfee and Windows Update. Workstations equipped with McAfee Agent software are automatically updated by the McAfee ePolicy Orchestrator (ePO) server every 30 minutes for new releases. Microsoft updates Windows® workstations monthly via a malicious software removal tool. We found workstation ADSF18C was missing Windows Malicious Software Removal Tool - October 2010 (KB890830) update. We were unable to run our security scan tests on workstation ADS9D43.	12a) The Windows Malicious Software Removal Tool should be updated for workstation ADSF18C, while also ensuring all other workstations are properly updated. 12b) For computer workstation ADS9D43, the ITSO should rerun, review, and correct all Malicious Code findings.	12a) This has been enabled and the computer was checked for malicious software. All computers are in the process of being evaluated. **Implementation Date**: Immediately 12b) The IT Security Office will rerun, review, and correct all Malicious Code findings. **Implementation Date**: Immediately
D.3 (see page 29)		Maturity Model: 4
Files are scanned when accessed only. Hard drive antivirus scanning is not performed due to performance degradation.	No recommendations.	
D.4 (see page 29)		Maturity Model: 4
Malicious code is quarantined when detected and deleted after 45 days. However, System Administrators are not alerted when malicious code is detected.	13) IT security group should be notified when malicious code is detected. Notifications should be grouped, evaluated and analyzed for root cause which may be used for continuous improvements.	13) EPO can be configured to send alerts on behaviors indicating the presence of malicious software. This feature needs to be tested prior to implementation. **Implementation Date**: April 30, 2011

Findings	Recommendations	Management Responses
D.5 (see page 29)		Maturity Model: 3
With regard to malicious code protection, we found no exceptions for workstation ADSF18C. For workstation ADS9D43, McAfee OAS is disabled.	14a) Root cause analysis should be performed on workstation ADS9D43. 14b) As the cause may affect additional workstations within the University, the results from the root cause analysis should be documented and distributed to appropriate parties to ensure all workstations are uniform.	14a) The analysis will be performed. **Implementation Date**: April 30, 2011 14b) Any workstations that could be affected will be addressed. **Implementation Date**: March 30, 2011
D.6 (see page 30)		Maturity Model: 4
Malicious Code Protection mechanisms are centrally managed by the ePO server.	No recommendations.	
D.7 (see page 30)		Maturity Model: 3
ADSF18C: Missing Windows Malicious Software Removal Tool – October 2010 (KB890830).	15a) For ADSF18C: Install latest Windows Malicious Software Removal Tool and a root cause analysis should be performed. 15b) The results from the root cause analysis should be documented and distributed to appropriate parties to ensure all workstations are uniform.	15a) The install will be performed and problem analyzed. **Implementation Date**: April 30, 2011 15b) The results will be addressed. **Implementation Date**: April 30, 2011
D.8 (see page 30)		Maturity Model: 3
Non-privileged users are not able to circumvent malicious code protection.	No recommendations.	

Appendix A - Control Objectives

The following information systems audit table represents a detailed analysis of the audit findings based upon the scope of the audit.

Control Objectives	Governance, Risk & Compliance Standards				Control Number(s)
User Account Management Identity Management Segregation Of Duties Workstation Security	COBIT	NIST	Regulation	Other	Controls applied
A. User Account Management					
1. Access Control Policies: (i) the access control policy should be developed and formally documented (ii) the access control policy should addresses: - purpose - scope - roles and responsibilities - legal and regulatory guidelines (iii) there should be a defined frequency of access control policy reviews/updates (iv) access control policies should be reviewed/updated in accordance within the University-defined frequency	Deliver and Support	sp 800-53A	FIU	AG Report No.2007-006	NIST AC-1.1 COBIT DS5.4 PantherSoft Financials Security Policy FIU PeopleSoft Grants Suite Implementation Security Role Handbook Auditor General Finding No.3

Control Objectives	Governance, Risk & Compliance Standards				Control Number(s)
User Account Management Identity Management Segregation Of Duties Workstation Security	COBIT	NIST	Regulation	Other	Controls applied
2. Access Control Procedures User account management should include: (i) establishing, activating, modifying, disabling, and removing accounts (ii) notifying account managers when temporary account are no longer required and when information system users are terminated, transferred, or application usage or need to know changes (iii) deactivating temporary accounts that are no longer required; and accounts of terminated or transferred users (iv) granting access to the application based on; a valid access authorization; intended application usage	Deliver and Support	Sp 800-53A	FIU	AG Report No.2007-006	NIST AC-2.1 NIST PS-4.1(i) COBIT DS5.4 FIU 1930.020a Auditor General Finding No.3
3. The University should automate mechanisms to support information system account management functions, including: (i) the University should have a defined time period for each type of account after which the information system terminates temporary and emergency accounts (ii) the application should automatically terminated temporary and emergency accounts after University-defined time period for each type of account (iii) University should define a time period after which inactive accounts are automatically disabled (iv) the application should automatically disable inactive accounts after University- defined time period	Deliver and Support	sp 800-53A			NIST AC-2(1).1 NIST AC-2(2).1 NISTAC-2(3).1 COBIT DS5.4

Control Objectives	Governance, Risk & Compliance Standards				Control Number(s)
User Account Management Identity Management Segregation Of Duties Workstation Security	COBIT	NIST	Regulation	Other	Controls applied
4. User Account Audit Trail: (i) the information system should automatically audit; account creation, modification, disabling, and termination actions (ii) the information system should notify, as required, appropriate individuals	Deliver and Support	sp 800-53A			COBIT DS5.4 NIST AC-2(4).1

Control Objectives	Governance, Risk & Compliance Standards				Control Number(s)
User Account Management Identity Management Segregation Of Duties Workstation Security	COBIT	NIST	Regulation	Other	Controls applied
5. Privilege User Accounts: (i) the University should establish and administer privileged user accounts in accordance with a role-based access scheme (ii) the University should track and monitor privileged role assignments	Deliver and Support	sp 800-53A		AG Report No.2007-006	COBIT DS5.4 NIST AC-2(7).1 Auditor General Finding No.3

B. Identity Management					
1. The University should manage information system accounts, including: (i) identifying account type (i.e., individual, group, system, application, custom, guest/anonymous, and temporary) (ii) establishing conditions for group membership (iii) identifying authorized users of the information system and specifying access privileges (iv) require appropriate approvals for requests to established accounts (v) specifically authoring and monitoring the use of guest/anonymous and temporary accounts	Deliver and Support	sp 800-53A		AG Report No.2007-006	COBIT DS5.3 NIST AC-2.1 Auditor General Finding No.3
2. Least Privilege Account Access: (i) The University should employ the concept of least privilege, allowing only authorized access for users (and process acting on behalf of users) which is necessary to accomplish assigned tasks in accordance with University missions and business functions. (ii) The information system should provide separate access selections to enable finer-grained allocation of user privileges (iii) The University should limits authorization to super user accounts on the information system to designated system administration personnel	Deliver and Support	sp 800-53A	FIU	AG Report No.2007-006	COBIT DS5.3 NIST AC-6.1 FIU_Security_Admin FIU_Security_Admin_LTD01 Auditor General Finding No.3

C. Segregation Of Duties					
1. The University should separate duties of individual users, as necessary, to prevent malevolent activity without collusion.	Plan and Organize	sp 800-53A	FIU	AG Report No.2007-006	FIU_BI_Specialist FIU_AR_Specialist FIU_BI_AR_Manager FIU_Security_Admin FIU_Security_Admin_LTD01 COBIT PO 4.11 NIST AC-5.1(i) Auditor General Finding No.3
2. The University should document separation of duties.	Plan and Organize	sp 800-53A	FIU		FIU PantherSoft Financials Security Policy FIU PeopleSoft Suite Implementation Security Role Handbook COBIT PO.4.11 NIST AC-5.1(ii)

3. Evaluate access to Key Navigations: (i) Identify key navigations. Determine which role | permission lists contain the key navigation (ii) For the identified roles | permission lists, determine whether the user's add |update access is appropriate for their job function	Plan and Organize		FIU	AG Report No.2007-006	COBIT PO4.12 COBIT PO4.13 FIU_BI_Specialist FIU_AR_Specialist FIU_BI_AR_Manager Auditor General Finding No.3
D. Workstation Security					
1. The University should employ at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code, including: (i) transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; (ii) inserted through the exploitation of information systems vulnerabilities	Deliver and Support	sp 800-53A	FIU	AG Report No.2007-006	COBIT DS5.9 NIST SI-3.1 FIU 1930.020c Auditor General Finding No.2
2. The University should update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy.	Deliver and Support	sp 800-53A			COBIT DS 5.9 NIST SI-3.1(iii)

3. The University should define the frequency of periodic scans of the information system by malicious code protection mechanisms.	Deliver and Support	sp 800-53A			COBIT DS5.9 NIST SI-3.1(iv)
4. The University should define one or more of the following actions to be taken in response to malicious code detection: (i) block malicious code (ii) quarantine malicious code; and or (iii) send alert to administrator	Deliver and Support	sp 800-53A			COBIT DS5.9 NIST SI-3.1(v)
5. The University should configure malicious code protection mechanisms to: (i) perform periodic scans of the information system in accordance with University-defined frequency; (ii) perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with University security policy; and (iii) take University-defined action(s) in response to malicious code detection	Deliver and Support	sp 800-53A			COBIT DS5.9 NIST SI-3.1(vi)

6. The University should centrally manage malicious code protection mechanisms.	Deliver and Support	sp 800-53A			COBIT DS5.9 NIST SI-3(1).1
7. The information system should automatically updates malicious code protection mechanisms, including signature definitions.	Deliver and Support	sp 800-53A			COBIT DS5.9 NIST SI-2(2).1
8. The information system should prevent non-privileged users from circumventing malicious code protection capabilities.	Deliver and Support	sp 800-53A			COBT DS5.9 NIST SI-3(3).1

Appendix B - COBIT Deliver and Support 5 Maturity Model Scoring Criteria Reference

DS5 Ensure Systems Security

Management of the process of Ensure systems security that satisfies the business requirements for IT of maintaining the integrity of information and processing infrastructure and minimizing the impact of security vulnerabilities and incidents is:

0 Non-existent: When the University does not recognize the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognizable system security administration process.

1 Initial/Ad Hoc: When the University recognizes the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive: When responsibilities and accountabilities for IT security are assigned to an IT security coordinator, although the management authority of the coordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analyzed. Services from third parties may not address the specific security needs of the University. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see IT security as within its domain.

3 Defined: When security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. Ad hoc security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business, but is only informally scheduled and managed.

4 Managed and Measurable: When responsibilities for IT security are clearly assigned managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and procedures are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorization are standardized. Security certification is pursued for staff members who are responsible for the audit and management of security. Security testing is completed using standard and formalized processes, leading to improvements of security levels. IT security processes are co-ordinated with an overall University security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and

managed in a manner that responds to business needs and defined security risk profiles. Goals and metrics for security management have been defined but are not yet measured.

5 Optimized: When IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimized and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalized incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of the implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analyzed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated University-wide. Metrics for security management are measured, collected and communicated. Management uses these measures to adjust the security plan in a continuous improvement process.

Appendix C - COBIT Plan and Organize 4 Maturity Model Scoring Criteria Reference

PO4 Define the IT Processes, University and Relationships

Define the IT processes that satisfy the business requirement for IT being agile in responding to the business strategy while complying with governance requirements and providing defined and competent points of contact is:

0 Non-existent: When the IT Department within the University is not effectively established to focus on the achievement of business objectives.

1 Initial/Ad Hoc: When IT activities and functions are reactive and inconsistently implemented. IT is involved in business projects only in later stages. The IT function is considered a support function, without an overall University perspective. There is an implicit understanding of the need for an IT University; however, roles and responsibilities are neither formalized nor enforced.

2 Repeatable but Intuitive when the IT function is organized to respond tactically, but inconsistently, to customer needs and vendor relationships. The need for a structured University and vendor management is communicated, but decisions are still dependent on the knowledge and skills of key individuals. There is an emergence of common techniques to manage the IT organization and vendor relationships.

3 Defined: When defined roles and responsibilities for the IT organization and third parties exist. The IT Department within the University is developed, documented, communicated and aligned with the IT strategy. The internal control environment is defined. There is formalization of relationships with other parties, including steering committees, internal audit and vendor management. The IT Department within the University is functionally complete. There are definitions of the functions to be performed by IT personnel and those to be performed by users. Essential IT staffing requirements and expertise are defined and satisfied. There is a formal definition of relationships with users and third parties. The division of roles and responsibilities is defined and implemented.

4 Managed and Measurable: When the IT Department, within the University, proactively responds to change and includes all roles necessary to meet business requirements. IT management, process ownership, accountability and responsibility are defined and balanced. Internal good practices have been applied in the University of the IT functions. IT management has the appropriate expertise and skills to define, implement and monitor the preferred department and relationships. Measurable metrics to support business objectives and user-defined critical success factors (CSFs) are standardized. Skill inventories are available to support project staffing and professional development. The balance between the skills and resources available internally and those needed from external UNIVERSITYs is defined and enforced. The IT Department within the University structure appropriately reflects the business needs by providing services aligned with strategic business processes, rather than with isolated technologies.

5 Optimized: When the IT Department, within the University structure, is flexible and adaptive. Industry good practices are deployed. There is extensive use of technology to assist in

monitoring the performance of the IT Department within the University and its processes. Technology is leveraged in line to support the complexity and geographic distribution of the University. There is a continuous improvement process in place.

Appendix D - Interviews and Acknowledgements

We would like to thank the following individuals for their cooperation and assistance during the audit:

- Larisa Goldberg, Assistant Director of Administrative Software
- Robert Grillo, Interim Vice President of Information Technology & CIO
- Carlos A. Flores, Director Operations and Systems, HR Administration
- Joseph R. Barabino, Associate Vice President Research Programs, Division of Research
- Aida Reus, Associate Director, Post Award Programs, Division of Research
- David W. Driesbach, Director University Computer Systems, Division of Research
- Mike R. Kirgan, Associate Director University Computer Systems, Operations
- Rexwell L Minnis, Coordinator Computer Systems Control, Operations
- Anu Chirinos, Coordinator Computer Systems Control, Operations
- Winny Lau, Computer Programmer-Analyst, Support Center, Field Team
- Joaquin Bello, Associate Controller, Financial Systems and Support Services
- Hamza Lazrak, Assistant Director, Financial Systems & Support Services
- Cheryl Granto, IT Security Officer
- Donna Day, Coordinator Computer Applications, IT Security Office
- Jonathan Broche, Student Assistant, IT Security Office
- Leyda Benitez, Associate Vice President Administration Affairs, University Compliance
- Rafael Figueroa, Manager Windows Systems Group, Operations & Enterprise Systems