REPORT NO. 2014-027
OCTOBER 2013

FLORIDA GULF COAST UNIVERSITY

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

BOARD OF TRUSTEES AND PRESIDENT

Members of the Board of Trustees and President who served during the 2012-13 fiscal year are listed below:

Robbie Roepstorff, Chair
Joseph Catti, Vice Chair
Juan Cubillo from 4-01-13 (1)
Peter Cuderman to 3-31-13 (1)
Dr. Shawn Felton from 6-01-13 (2)
J. Dudley Goodlette from 1-17-13
Ann Hamilton
Dr. Douglas Harrison to 5-31-13 (2)
Richard Klaas from 5-31-13 (3)
Dr. John Little
Scott F. Lutgert
Dorene McShea
Edward Morton to 1-10-13 (4)
Russell Priddy
Christian Spilker from 5-31-13 (4)
Doug St. Cerny to 1-16-13
Robert Wells

Dr. Wilson G. Bradshaw, President

Notes: (1) Student body president.
(2) Faculty senate chair.
(3) Position was vacant from July 1, 2012, through May 30, 2013
(4) Position was vacant from January 11, 2013, through May 30, 2013

The audit was conducted by Deirdre F. Waigand, CPA. For the information technology portion of this audit, the audit team leader was Deidre Melton, CISA, and the supervisor was Heidi G. Burns, CPA, CISA. Please address inquiries regarding this report to James R. Stultz, CPA, Audit Manager, by e-mail at jimstultz@aud.state.fl.us or by telephone at (850) 412-2869.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

FLORIDA GULF COAST UNIVERSITY

EXECUTIVE SUMMARY

Our operational audit disclosed the following:

INFORMATION TECHNOLOGY

Finding No. 1: Some inappropriate or unnecessary information technology (IT) access privileges existed, indicating a need for an improved review of access privileges.

Finding No. 2: The University lacked written policies and procedures for the configuration and management of file transfer protocol sites.

Finding No. 3: University IT security controls related to user authentication, data loss prevention, and logging and monitoring of network security events needed improvement.

BACKGROUND

Florida Gulf Coast University (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors. The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the Board of Governors appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered terms of five years. The faculty senate chair and student body president also are members.

The Board of Governors establishes the powers and duties of the Trustees. The Trustees are responsible for setting University policies, which provide governance in accordance with State law and Board of Governors' Regulations. The University President is selected by the Trustees and confirmed by the Board of Governors. The University President serves as the executive officer and the corporate secretary of the Trustees and is responsible for administering the policies prescribed by the Trustees for the University.

The results of our financial audit of the University for the fiscal year ended June 30, 2013, will be presented in a separate report. In addition, the Federal awards administered by the University are included within the scope of our Statewide audit of Federal awards administered by the State of Florida and the results of that audit, for the fiscal year ended June 30, 2013, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Information Technology

Finding No. 1: Access Privileges

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls provide employees access to IT resources based on a demonstrated need to view, change, or delete data and restrict employees from performing incompatible functions or functions inconsistent with their areas of responsibilities. For example, access privileges should typically be configured to enforce a separation of IT and application end-user duties whereby only the responsible end-users can originate or correct transactions and initiate changes to data files and IT employees are restricted from performing end-user functions. Periodic reviews of access privileges are necessary to ensure that employees can only access IT

resources that are necessary to perform their assigned job duties and that the assigned access privileges enforce an appropriate separation of incompatible duties.

Our test of selected access privileges to the University's Enterprise Resource Planning (ERP) system, including finance and human resources (HR) applications, the supporting database, and host operating system, disclosed some access privileges that were unnecessary or that permitted employees to perform incompatible functions. Specifically:

- Seven business technology services employees and one employee from the University's host data center had update access privileges to all critical transactions within the ERP finance and HR applications. The access privileges granted were contrary to an appropriate separation of end-user duties and the employees' assigned IT duties related to the technical support of the University ERP applications. .
- The director of procurement had update access privileges to critical transactions within the ERP finance application, including creating or modifying vendors, purchase orders, invoices, and journal entries and processing electronic funds transfers and manual checks. In addition, an HR coordinator had update access privileges to critical transactions within the ERP HR application, including inputting employees and rates of pay, modifying employee address information, and entering time and pay adjustments. These privileges permitted the employees to perform incompatible duties and, upon our inquiry, University management acknowledged that some of the privileges assigned were unnecessary for the employees' assigned job duties.
- Three database administrators and three database administrators with the University's host data center had unnecessary update access to one database account used for creating custom tables and stored procedures, and another ERP-delivered account used in payroll processing, with update access privileges to all critical finance and HR transactions.
- Three database administrators and three database administrators with the University's host data center had update access to two database accounts with database administrator privileges that were no longer used for University operations. Inactive accounts may not have appropriate user database authentication controls in effect or be monitored for use, increasing the risk of compromise.
- Sixteen employee accounts had administrator access privileges to the operating system supporting the ERP database allowing complete access to the database. Seven of the accounts were assigned to former University employees and nine of the accounts were assigned to employees no longer having responsibilities for the operating system administration.

Although the University had compensating controls in place (e.g., reviewed ERP access privileges quarterly and developed a procedure to begin reviewing network access) to help mitigate the effect of the inappropriate or unnecessary access privileges noted above, the existence of the inappropriate or unnecessary access privileges indicated a need for an improved review of access privileges and increased the risk of unauthorized disclosure, modification, or destruction of University data and IT resources.

Recommendation: The University should improve its review of IT access privileges to include all access privileges and remove inappropriate or unnecessary access detected to ensure that access privileges are compatible with assigned job duties.

Finding No. 2: Written Policies and Procedures

Effective security controls include configuring and managing all levels of the computing environment to ensure against unauthorized access or exploitable vulnerabilities. File transfer protocol (FTP) services are used to transfer files over a network providing for the exchange of data between entities. Because of the critical or sensitive nature of the data that may be included on an FTP site, written policies and procedures are necessary to document the configuration requirements and provide benchmarks against which to monitor and manage security. Such requirements should include disabling of default accounts, logging and monitoring of the site, establishing user

accounts and restricting access, limiting the availability of files, setting authentication parameters, and implementing encryption standards.

Although the University had various FTP sites established, the University had not developed written policies and procedures for the authorization, creation, and maintenance of accounts and the monitoring of files placed on FTP sites. Without written policies and procedures, the University's FTP sites may not be configured and managed consistently, increasing the risk that the confidentiality, integrity, and availability of University data may be compromised.

Recommendation: The University should establish written policies and procedures for the configuration and management of FTP sites.

Finding No. 3: Security Controls - User Authentication, Data Loss Prevention, and Logging and Monitoring of Network Security Events

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that certain University security controls related to user authentication, data loss prevention, and logging and monitoring of network security events needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising University data and IT resources. However, we have notified appropriate University management of the specific issues. Without adequate security controls related to user authentication, data loss prevention, and logging and monitoring of network security events, the risk is increased that the confidentiality, integrity, and availability of University data and IT resources may be compromised. A similar finding related to user authentication controls was noted in our report No. 2011-011.

Recommendation: The University should improve security controls related to user authentication, data loss prevention, and logging and monitoring of network security events to ensure the continued confidentiality, integrity, and availability of University data and IT resources.

PRIOR AUDIT FOLLOW-UP

The University had taken corrective actions for findings included in our report No. 2011-011, except security controls over user authentication noted in finding No. 3 was also noted in prior audit report No. 2011-011, as finding No. 2.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this operational audit from March 2013 to August 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this operational audit were to:

- Evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines.
- Examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, reliability of records and reports, safeguarding of assets, and identifying weaknesses in those controls.
- Determine whether management had taken corrective actions for findings included in our report No. 2011-011.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for those programs, activities, or functions included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular transactions, legal compliance matters, records, and controls considered.

For those programs, activities, and functions included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the program, activity, or function; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

The scope and methodology of this operational audit are described in Exhibit A. Our audit included the selection and examination of records and transactions occurring during the 2012-13 fiscal year. Unless otherwise indicated in this report, these records and transactions were not selected with the intent of projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

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 operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

Management's response is included as Exhibit B.

EXHIBIT A
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Information technology (IT) logical assess controls and user authentication.	Reviewed selected operating system, database, network, and application security settings to determine whether authentication controls were configured and enforced in accordance with IT best practices.
IT access privileges and separation of duties.	Reviewed procedures for maintaining and reviewing access to IT resources. Tested selected access privileges over the operating system, database, network, and Enterprise Resource Planning applications to determine the appropriateness and necessity based on the employees' job duties and user account functions and adequacy with regard to preventing the performance of incompatible duties.
IT logging and monitoring.	Reviewed procedures and reports related to the capture, review, maintenance, and retention of selected system and security event logs.
IT policies and procedures.	Reviewed the University's written IT policies and procedures to determine whether they addressed certain important IT control functions.
IT data loss prevention.	Reviewed the University's written security policies, procedures, and programs in effect governing the classification, management, and protection of sensitive and confidential information.
IT security incident response.	Reviewed the University's written policies and procedures, plans, and forms related to security incident response and reporting.
Board and committee meetings.	Reviewed Board and committee minutes to determine whether Board approval was obtained for policies and procedures in effect during the audit period and for evidence of compliance with Sunshine law requirements (i.e., proper notice of meetings, ready access to public, and maintenance of minutes).
Textbook affordability.	Examined supporting documentation to determine whether the University's procedures regarding textbook affordability were in accordance with Section 1004.085, Florida Statutes.
Internal audit function (inspector general).	Reviewed the internal audit function to determine whether the University followed professional requirements and provided for peer review of reports issued.
Investments.	Determined whether the Board established investment policies and procedures as required by Section 218.415, Florida Statutes, and whether investments during the fiscal year were in accordance with those policies and procedures.

EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Student receivables.	Determined whether student receivables were properly authorized, documented, and properly recorded. Determined adequacy of collection efforts and whether uncollectable accounts written-off were properly approved. Determined whether restrictions on student records and holds on transcripts and diplomas were adequate and enforced for delinquent accounts.
Florida residency determination and tuition.	Tested student registrations to determine whether the University documented Florida residency and correctly assessed tuition in compliance with Sections 1009.21, 1009.24, and 1009.286(2), Florida Statutes, and Board of Governors Regulation 7.005.
Tuition differential fees.	Reviewed payments from tuition differential fees collected to determine whether the University assessed and used tuition differential fees in compliance with Section 1009.24(16)(a), Florida Statutes.
Terminal pay.	Reviewed the University's policies and procedures for terminal pay to ensure consistency with Florida law. Tested former employees to determine appropriateness of terminal pay.
Severance pay.	Reviewed severance pay provisions in selected contracts to determine whether the University was in compliance with Florida Statutes.
Administrative employees' compensation.	Reviewed administrative employees' compensation to determine whether compensation did not exceed limits provided in Florida law.
President's compensation.	Determined whether the President's compensation was in accordance with Florida law, Board of Governors Regulations, and University policy.
Bonuses.	Determined whether employee bonuses were paid in accordance with Section 215.425(3), Florida Statutes.
Electronic funds transfers and payments.	Reviewed University policies and procedures related to electronic funds transfers and payments. Tested supporting documentation to determine whether selected electronic funds transfers and payments were properly authorized and supported.
Purchasing card transactions.	Tested transactions to determine whether purchasing cards were administered in accordance with University policies and procedures. Also, tested former employees to determine whether purchasing cards were timely cancelled upon termination of employment.
Travel expenses.	Tested executive foreign and out-of-state travel expenses to determine whether the travel was reasonable, adequately supported, and for University purposes.

EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Contractual agreements.	Determined whether contractual services were supported by Board-approved contracts. Also, examined and tested the aforementioned contracts to determine whether the contracts were properly awarded and executed, contract terms were adequately supported, and vendors carried adequate insurance.
Construction administration.	For selected major construction projects, tested payments and supporting documentation to determine compliance with University policies and procedures and provisions of laws and rules. Also, for construction management contracts, determined whether the University monitored the selection process of architects and engineers, construction managers, and subcontractors by the construction manager.
Direct-support organizations – conflicts of interest.	Determined whether the University had established policies and procedures to avoid potential conflicts of interest with vendors who were doing business with the University and made donations to the University's direct-support organizations.
Procedures for athletic department's athletic camps	Tested athletic camps and reviewed supporting documentation for cash collections and employee compensation.

EXHIBIT B
MANAGEMENT'S RESPONSE

FLORIDA GULF COAST UNIVERSITY

Office of the Vice President
Administrative Services and Finance Office

October 14, 2013

Mr. David W. Martin
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

RE: Florida Gulf Coast University
Operational Audit

Please find attached Florida Gulf Coast University's (FGCU) written response to the preliminary and tentative findings and recommendation resulting from the Operational Audit for the fiscal year ended June 30, 2013.

Pursuant to Section 11.45(4)(d), Florida Statues, FGCU submits this written response with a statement of explanation concerning the findings including actual or proposed corrective action as appropriate to each of the three Information Technology findings.

As always, we appreciate the work of the Auditor General and welcome further discussion on any of the proposed findings and recommendations.

If you have any questions regarding the ability to access and read the attached PDF file, please contact Ms. Linda Bacheler at (239) 590-1212.

Sincerely,

Steve L. Magiera CPA, MS
Vice President
Administrative Services and Finance
Florida Gulf Coast University

(239) 590-1100 FAX: (239) 590-1010 http://www.fgcu.edu
10501 FGCU Boulevard South • Fort Myers, Florida 33965-6565
An Affirmative Action Equal Opportunity Employer • A member of the State University System of Florida

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Gulf Coast University
Response to Operational Audit Recommendations
For the Fiscal Year Ended June 30, 2013

Recommendation No 1:
The University should improve its review of IT access privileges to include all access privileges and remove inappropriate or unnecessary access detected to ensure that access privileges are compatible with assigned job duties.

RESPONSE:
The University agrees there is a need to review IT access privileges and was in the process of evaluating employee needs based upon current job classification and consolidation security classes prior to the audit inquiry. During the audit inquiry, all access privileges brought to the University's attention were removed or adjusted, however, the University will continue to evaluate employee needs to determine the correct security classes. Being a small University with limited staff to perform multiple tasks, the University has implemented very strong compensating controls and reports to mitigate the risk of control deficiencies and has not experienced unauthorized disclosure, modification, or destruction of University data and IT resources. To further strengthen ERP controls, the quarterly review process of access privileges is undergoing an extensive evaluation to enhance manageability of appropriate and necessary employee privileges.

IMPLEMENTATION DATE: Sensitive systems - December 2013, less sensitive systems June 2014.

AUDITEE: Mary Banks, Assistant VP Business Technology Services

Recommendation No 2:
The University should establish written policies and procedures for the configuration and management of FTP sites.

RESPONSE:
The University agrees with the recommendation and will continue to strengthen the procedures in place for documenting configuration requirements, access control and monitoring of FTP site activity with written policies and procedures to ensure compliance.

IMPLEMENTATION DATE: March 2014

AUDITEE: Mary Banks, Assistant VP Business Technology Services

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation No 3:
The University should improve security controls related to user authentication, data loss prevention, and logging and monitoring of network security events to ensure the continued confidentiality, integrity, and availability of University data and IT resources.

RESPONSE:
The University acknowledges this finding and will continue to seek solutions that improve our information security program. The University made some immediate improvements to address the concerns raised during the audit which had previously been identified by the University as areas for further evaluation. Specifically, user's authentication is in place and policies for a data loss and prevention program are in the final stages of implementation. The University is currently developing and implementing additional security controls related to logging and monitoring of network security events. The University will continue to review and explore additional security controls to ensure confidentiality, integrity, and availability of University data and IT resources.

IMPLEMENTATION DATE: Ongoing

AUDITEE: Mary Banks, Assistant VP Business Technology Services