REPORT NO. 2013-054
DECEMBER 2012

COLLEGE OF CENTRAL FLORIDA

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

BOARD OF TRUSTEES AND PRESIDENTS

Members of the Board of Trustees and Presidents who served during the 2011-12 fiscal year are listed below:

	County
Cory Pool, Chair	Marion
Ronald Ewers, Vice Chair	Marion
Sandra Balfour	Citrus
Joyce Brancato	Levy
Robert Durrance	Levy
Priya Ghumman	Marion
Don Taylor	Citrus

Dr. James D. Harvey, Interim President
to December 31, 2011

Dr. James D. Henningsen, President
from January 1, 2012

The audit team leader was G. Christian Meyer, CPA, and the audit was supervised by Philip B. Ciano, CPA. For the information technology portion of this audit, the audit team leader was Shawn McCormick, 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) 922-2263.

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) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

COLLEGE OF CENTRAL FLORIDA

SUMMARY

Our operational audit disclosed the following:

BOARD POLICIES

Finding No. 1: The Board needs to enhance its written policies and procedures relating to electronic funds transfers.

PERSONNEL AND PAYROLL

Finding No. 2: The College President's employment agreement included a severance pay provision that was contrary to Section 215.425(4)(a), Florida Statutes.

CONSTRUCTION ADMINISTRATION

Finding No. 3: The College needed to more frequently solicit architectural services.

INFORMATION TECHNOLOGY

Finding No. 4: Improvements were needed in College access controls to ensure that information technology (IT) access privileges were appropriately assigned.

Finding No. 5: The IT access privileges of some former College employees were not timely deactivated.

Finding No. 6: Contrary to the requirements of the State of Florida *General Records Schedule*, the College did not retain some IT access control records.

Finding No. 7: The College did not have a written IT security incident response plan.

Finding No. 8: College IT security controls related to user authentication, data loss prevention, and logging needed improvement.

BACKGROUND

The College of Central Florida (College) is under the general direction and control of the Florida Department of Education, Division of Florida Colleges, and is governed by State law and State Board of Education rules. A board of trustees (Board) governs and operates the College. The Board constitutes a corporation and is composed of seven members appointed by the Governor and confirmed by the Senate. The College President serves as the executive officer and the corporate secretary of the Board, and is responsible for the operation and administration of the College.

The College has its main campus, a special-purpose center, and a museum located in Ocala, Florida; a campus located in Lecanto, Florida; and a special-purpose center located in Chiefland, Florida. Additionally, credit and noncredit classes are offered in various physical locations throughout Citrus, Levy, and Marion Counties, and the College offers e-Learning courses through the Internet. The College reported enrollment of 6,514 full-time equivalent students for the 2011-12 fiscal year.

The results of our financial audit of the College for the fiscal year ended June 30, 2012, will be presented in a separate report. In addition, the Federal awards administered by the College 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, 2012, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Board Policies

Finding No. 1: Electronic Funds Transfers

Section 1010.11, Florida Statutes, requires each college board of trustees to adopt written policies prescribing the accounting and control procedures under which funds are allowed to be moved by electronic transaction for any purpose including direct deposit, wire transfer, withdrawal, investment, or payment. This law also requires that electronic transactions comply with the provisions of Chapter 668, Florida Statutes, which discusses the use of electronic signatures in electronic transactions between colleges and other entities.

According to College records, $88 million in outgoing electronic funds transfers were made during the 2011-12 fiscal year. The Board has adopted a policy that provides that the Board may establish rules to authorize by electronic medium the receipt or transfer of public funds to, from, or within its established bank accounts for purposes of investment or direct deposit of funds provided adequate internal controls are maintained. However, the Board policy does not address the accounting and control procedures related to electronic funds transfers or the use of electronic signatures, contrary to the above-cited laws. The College did establish an Administrative Procedure that requires each department that performs electronic or telephonic funds transfers to develop written procedures that provide internal control measures, require that the departmental procedures be approved by the Chief Business Officer (CBO), and that the procedures be reviewed annually and updated as necessary, and whenever possible that two people be involved in each transfer, one to initiate the transfer and one to approve the transfer.

Our review indicated that four College departments that transfer funds developed written procedures and the Assistant Vice President of Finance (the CBO) performs an annual review of the procedures; however, neither the Administrative Procedure nor the departmental procedures were submitted to the Board for approval. While the College had established controls over electronic funds transfers, the lack of specific guidance in the Board policy increases the risk that electronic funds transfers will not be executed in accordance with Board directives and the provisions of Chapter 668, Florida Statutes.

Recommendation: The Board should enhance its policy to address accounting and control procedures for electronic funds transfers, including the use of electronic signatures.

Personnel and Payroll

Finding No. 2: President's Employment Agreement

Section 215.425(4)(a), Florida Statutes, provides that on or after July 1, 2011, a unit of government that enters into a contract or employment agreement, or renewal or renegotiation of an existing contract or employment agreement, that contains a provision for severance pay with an officer, agent, employee, or contractor must include certain provisions, including a provision that severance pay may not exceed an amount greater than 20 weeks of compensation.

On October 25, 2011, the Board approved an employment agreement with the new College President. The terms of the employment agreement provide for a three-year period commencing on January 1, 2012, through December 31, 2014. Paragraph 9.4 of the employment agreement provides that in the event that the President is

discharged without cause, the President will be paid up to one year's base salary from appropriated State funds. This provision is contrary to Section 215.425(4)(a), Florida Statutes, in that it allows for the possibility of the President receiving severance pay that exceeds 20 weeks of salary.

Recommendation: The College should ensure that future employment agreements contain provisions for severance pay that are in accordance with Section 215.425(4)(a), Florida Statutes. The College should also take appropriate action to amend the President's employment agreement to be consistent with Section 215.425(4)(a), Florida Statutes.

Construction Administration

Finding No. 3: Continuing Contracts

The effective utilization of a competitive selection processes when obtaining professional services provides assurance to the public that the College's selection of service providers is fair, equitable, and provides for the most economical procurement of services. Fair and open competition is a basic tenet of public procurement and such competition reduces the appearance and opportunity for favoritism and inspires public confidence that contracts are awarded equitably and economically.

In October 2003, the Board entered into a contract with an architect for College-wide renovations and remodeling projects on a continuing basis. The contract was for a period of three years, then provided for automatic annual renewals beginning in October 2006 unless notice was given by either party a minimum of 90 days prior to each anniversary date. According to the contract, compensation to the architect for basic services was based on Florida Department of Management Services, Division of Building Construction fee schedules. In addition, the contract allowed fees for additional services beyond the basic services at hourly rates ranging from $35 per hour for clerical personnel to $120 an hour for personnel classified as principal, and the fees were subject to review for possible adjustment at the time of the annual contract extensions. Fees for additional services increased five percent each year as the agreement was renewed in 2006, 2007, 2008, and 2009, a cumulative increase of approximately 21.5 percent. There were no increases in the fees for 2010, 2011, or 2012 for the additional services. Payments to the architect from October 2006 through June 2012 for basic and additional services totaled approximately $792,000. In October 2012, nine years after inception of the contract, the contract automatically renewed for another year. Since 2003, the College has not issued a solicitation to determine if any firms are willing to provide architectural services for College-wide renovations and remodeling projects at a lesser cost.

Periodic solicitation of architectural services would provide the College assurance that it is obtaining the lowest and best price consistent with desired quality, and would provide the public assurance that the College's selection process is fair, equitable, and provides for the economical procurement of architectural services.

Recommendation: The College should consider competitively selecting architectural service providers on a periodic basis to evidence that such services are obtained at the lowest and best price consistent with desired quality.

Information Technology

Finding No. 4: Access Privileges

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosures, modification, or destruction. Effective IT 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 outside of their areas of responsibility. Periodically reviewing assigned IT access privileges promotes good internal control and is necessary to ensure that employees cannot access or modify IT resources inconsistent with their assigned job responsibilities.

Our audit disclosed that improvements were needed in granting access privileges to certain IT resources, as follows:

- IT access privileges within the College's finance, human resources, and financial aid application were controlled by assigning employees access to menus and groups. The menus and groups assigned were stored in each employee's individual login directory; however, the College could not, upon audit request, provide a listing of all menus and groups assigned to each employee because, according to College management, of the difficulty in extracting access information from operating system files. Consequently, College records did not demonstrate the appropriateness of employee IT access privileges assigned within the application or that it had an effective process in place for maintaining and reviewing employee access to the application. Absent the ability to review access privileges, there is an increased risk that the College may not maintain appropriate security over the application or timely detect and address inappropriate or unnecessary access privileges, should they exist.
- One IT support account in the College's network and database supporting the finance, human resources, and financial aid applications had domain administrator privileges. This level of access was unnecessary for the intended purpose of the IT support account. Additionally, two database accounts had been assigned a database administrator role that included privileges unnecessary for the job responsibilities of the employees to whom the accounts had been assigned. In response to our inquiry, College management removed the IT support account from the domain administrators group on the network. When access privileges are unnecessarily granted or result in an inappropriate separation of duties, the risk is increased that unauthorized or unintentional network and database hardware, software, or configuration changes may occur and not be timely detected.

Recommendation: The College should implement procedures for the periodic review of access privileges and remove any inappropriate or unnecessary access detected.

Finding No. 5: Timely Deactivation of Access Privileges

Effective IT access controls include provisions for the timely deactivation of employee access privileges when employment terminations occur. Prompt action is necessary to ensure that former employees' access privileges are not misused by the former employees or others.

According to the College's *Information Security Procedures*, when an employee leaves the College, the employee's immediate supervisor and the human resources department are to notify the IT department for part- and full-time employees, respectively. The removal or deactivation of access privileges to the College's network prevents the former employee from being able to access the finance, human resources, and financial aid applications. The College's procedures provided for privileges associated with the employee to be removed and the College's practice was to deactivate both the network and application user accounts.

Our test of 22 former College employees who had terminated employment during the period July 1, 2011, through February 2, 2012, disclosed the following as of April 5, 2012:

- The finance, human resources, and financial aid applications' access privileges of five former employees, including two who were deceased, were not deactivated for 32 to 202 days after termination of employment, contrary to the College's *Information Security Procedures*.
- The network access privileges of two former employees remained active for 237 days after termination of employment. Additionally, the network access privileges of one of the deceased employees referenced above remained active for 201 days. The College's network allows access to certain critical application systems and confidential or sensitive information stored with documents of individual network users. In response to our inquiry, College management indicated that the three network accounts remaining active had been deleted; however, because there was no longer an access control record, the College was unable to determine the date the accounts were deactivated. In addition, for one of the employees whose application access privileges had not been timely deactivated, there was not an access control record available related to her network access privileges, including the deactivation date and last log-in date (see finding No. 6).

Subsequent to our inquiry, the College determined that the last sign-on of the former employees using the network and application user accounts occurred on or prior to the date of termination with the exception of two employee network accounts that had been deleted. When the access privileges of former employees are not timely deactivated, the risk is increased that the access privileges may be misused by the former employees or others.

Recommendation: The College should ensure that access privileges of former employees are deactivated in a timely manner.

Finding No. 6: Access Control Records Retention

The State of Florida *General Records Schedule GS1-SL for State and Local Government Agencies (General Records Schedule)*, revised by the Department of State effective August 2010, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment. In accordance with the College's *Information Security Procedures*, a former employee's network account may be available to the employee's supervisor for 90 days for purposes of reviewing e-mail. Although not part of the written procedure, the College's practice was to delete some of the network accounts following the 90-day period, contrary to the *General Records Schedule* requirements.

Without adequate retention of access control records, the risk is increased that the College may not have sufficient documentation to assist in future investigations of security incidents, should they occur. Additionally, the College is not in compliance with the State's record retention requirements.

Recommendation: The College should ensure that access control records are retained as required by the *General Records Schedule*.

Finding No. 7: Security Incident Response Plan

Computer security incident response plans are established by management to ensure an appropriate, effective, and timely response to security incidents. These written plans typically detail responsibilities and procedures for identifying, logging, and analyzing security violations and include a centralized reporting structure, provisions for designated staff to be trained in incident response, and notification to affected parties.

Although the College's *Information Security Procedures* states the IT Department is responsible for organizing responses to computer security incidents and tasks information owners with reviewing reports about system intrusion and other events relevant to their information, the College had not developed a written security incident response plan. Should an event occur that involves the potential or actual compromise, loss, or destruction of College data or IT resources, the lack of a written security incident response plan may result in the College's failure to take appropriate actions in a timely manner to prevent further loss or damage to College data and IT resources.

In response to our inquiry, College management indicated that a best practices information security framework developed by International Business Machines under contract with the Florida College System composed of 28 Florida colleges, including the College of Central Florida and the College Center for Library Automation, may be used as a basis for strengthening its written security incident response procedures.

Recommendation: The College should develop a written security incident response plan to provide reasonable assurance that the College will respond in a timely and appropriate manner to events that may jeopardize the confidentiality, integrity, or availability of data and IT resources.

Finding No. 8: Security Controls – User Authentication, Data Loss Prevention, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain College security controls related to user authentication, data loss prevention, and logging and monitoring that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising College data and IT resources. However, we have notified appropriate College management of the specific issues. Without adequate security controls related to user authentication, data loss prevention, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of College data and IT resources may be compromised.

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

PRIOR AUDIT FOLLOW-UP

The College had taken corrective actions for findings included in our report No. 2011-023.

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 2012 to October 2012 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, and the safeguarding of assets, and identify weaknesses in those controls.
- Determine whether management had taken corrective actions for findings included in our report No. 2011-023.
- 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 various records and transactions occurring during the 2011-12 fiscal year. Unless otherwise indicated in this report, these records and transactions were not selected with the intent of statistically 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) policies and procedures.	Reviewed the College's written IT policies and procedures to determine whether they addressed certain important IT control functions.
IT access privileges and separation of duties.	Reviewed procedures for maintaining and reviewing access to IT resources. Tested access privileges to determine the appropriateness based on the employees' job functions and responsibilities and adequacy with regard to preventing the performance of incompatible duties.
Deactivation of employee IT access.	Reviewed procedures to prohibit former employees' access to electronic data files.
IT security awareness and training.	Determined whether a comprehensive IT security awareness and training program was in place.
IT logging and monitoring.	Reviewed supporting documentation to determine whether logging and monitoring controls were in place in accordance with IT best practices.
IT data loss prevention.	Reviewed written policies, procedures, and programs in effect governing the classification, management, and protection of sensitive and confidential information.
IT security incident response.	Determined whether the College had developed an adequate written security incident response plan.
IT authentication controls.	Reviewed supporting documentation to determine whether authentication controls were configured and enforced in accordance with IT best practices.
Board and other meetings (workshops, interviews with Presidential candidates).	Reviewed Board minutes to determine compliance with Sunshine law requirements (i.e., proper notice of meetings, ready access to public, maintain minutes).
Fraud policy and related procedures.	Examined written policies and procedures related to the College's fraud policy and related procedures.
Social security number requirements of Section 119.071(5)(a), Florida Statutes.	Examined supporting documentation to determine whether the College had provided individuals with a written statement of the purpose of collecting their social security numbers.
Identity theft prevention program (Red Flags Rule).	Reviewed the College's policies and procedures related to its identity theft prevention program for compliance with the Federal Trade Commission's Red Flags Rule.
Student loans.	Determined whether the College had established procedures for students that transferred from other institutions of higher education, to verify whether the student was not in default on student loans or was not past due on a student receivable.
Florida residency determination and tuition.	Tested student registrations to determine whether the College documented Florida residency as required by Section 1009.21, Florida Statutes, and State Board of Education Rule 6A-10.044, Florida Administrative Code.

EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Distance learning on-line registration process for transient students.	Determined whether the on-line registration process for transient students was in compliance with Section 1004.091(2)(b), Florida Statutes.
Laboratory and other user fees.	Reviewed the College's procedures and determined whether they were approved by the Board of Trustees. Tested laboratory and other user fees and examined supporting documentation to determine whether the College properly calculated these fees.
Textbook affordability.	Examined supporting documentation to determine whether the College's policies and procedures regarding textbook affordability were in accordance with Section 1004.085, Florida Statutes.
Overtime payments.	Reviewed College policies, procedures, and supporting documentation evidencing the approval of, and necessity for, overtime payments. Reviewed overtime payments to determine the reasonableness of amounts paid.
Terminal pay.	Reviewed the College's rules and procedures for terminal pay to ensure consistency with Florida law. Tested former employees to determine appropriateness of terminal pay. Additionally, reviewed severance pay provisions in contracts entered into after July 1, 2011, to determine whether the College was in compliance with Florida Statutes.
Administrative employees' compensation.	Reviewed administrative employees' compensation to determine whether compensation exceeded limits provided in Florida law.
Presidents' compensation.	Determined whether the Presidents' compensation was in accordance with Florida law, rules, and Board policies.
Bonuses.	Determined whether employee bonuses were paid in accordance with Section 215.425(3), Florida Statutes.
Purchasing card transactions.	Tested transactions to determine whether purchasing cards were administered in accordance with College policies and procedures. Also, tested former employees to determine whether purchasing cards were timely cancelled upon termination of employment.
Travel expenses.	Tested executive foreign, out-of-State, and in-State travel expenses to determine whether the travel was reasonable, adequately supported, and for College purposes.
Contractual agreements.	Determined whether contractual services were supported by appropriately approved contracts. Also, examined and tested the aforementioned contracts to ensure that they were properly awarded and executed, that contract terms were adequately supported. Also determined whether there was sufficient documentation to evidence services were rendered prior to payment.
Payments to design professionals.	Reviewed payments to architect to determine appropriate payment of fees and related expenses.

EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Florida College System Program Fund.	Reviewed expenditures from the Florida College System Program Fund to ensure such funds were not expended on the education of State or Federal inmates.
Earmarked capital project resources.	Determined, on a test basis, whether Public Education Capital Outlay and other restricted capital outlay expenditures were expended in compliance with the restrictions imposed on the use of these resources.
State-funded capital outlay program reporting.	Determined whether amounts reported to the Florida Department of Education for State-funded capital outlay programs were supported by the College's accounting records.
Insuring architects and engineers.	Determined whether the Board had adopted a policy establishing minimum insurance coverage requirements for design professionals, such as architects and engineers. Examined documentation to determine whether engaged design professionals provided evidence of the required insurance.
Electronic funds transfers (EFTs), automated clearing house (ACH) withdrawals, and electronic vendor payments.	Reviewed College policies and procedures related to EFTs, ACH withdrawals, and electronic vendor payments to determine compliance with law and College policies and procedures. Tested supporting documentation for selected transactions to determine whether they were properly authorized and supported.
Enrollment reporting.	Performed analytical procedures related student enrollment to determine consistency and accuracy of enrollment information reported to the Florida Department of Education.
Adult general education program enrollment reporting.	Examined supporting documentation on a test basis to determine whether the College reported instructional and contact hours in accordance with Florida Department of Education requirements.
Cost analysis report.	Reviewed the College's annual Cost Analysis Report (CA-2) and supporting documentation to determine the report was properly prepared and agreed to College records.
Direct-support organizations – conflicts of interest.	Determined whether the College had established policies and procedures to avoid potential conflicts of interest with vendors who were doing business with the College and made donations to the College's direct-support organization.

EXHIBIT B
MANAGEMENT'S RESPONSE

College of Central Florida

Office of the President

December 7, 2012

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

Dear Mr. Martin:

The following is our response to the preliminary and tentative findings in the Operational Audit for College of Central Florida for the Fiscal Year Ended June 30, 2012.

Finding No. 1: The Board needs to enhance its written policies and procedures relating to electronic funds transfers.

The College has Board Policy 5.02 and the related Administrative Procedure in place that addresses electronic funds transfers and the establishment "of detailed written procedures that will provide adequate internal control measures that will insure the safety of the College's funds." In fact, the Auditor acknowledges in the finding, "The College did establish an Administrative Procedure that requires each department that performs electronic or telephonic funds transfers to develop written procedures that provide internal control measures, require that the departmental procedures be approved by the Chief Business Officer (CBO), and that the procedures be reviewed annually and updated as necessary, and whenever possible that two people be involved in each transfer, one to initiate the transfer and one to approve the transfer." At issue is the amount of detail contained in the Administrative Procedure that should be included in the Board Policy.

While the College feels the existing combination of policy and procedure has us in compliance with the spirit of the law and appropriately blends the policy making role of the Board and the operational responsibility of the administration, we will propose an amendment to the Board Policy 5.02 adding language to more specifically direct administration on requirements that should be contained in the electronic transfer of funds procedures.

Finding No. 2: The College President's employment agreement included a severance pay provision that was contrary to Section 215.425(4)(a), Florida Statutes.

3001 SW College Road • Ocala, Florida 34474-4415
Phone: 352-873-5835 • Fax: 352-873-5847 • E-mail: jim.henningsen@cf.edu
– an equal opportunity college –

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

As of December 4, 2012, the College's District Board of Trustees approved amendments to the President's employment agreement to be consistent with the above referenced statute.

Finding No. 3: The College needed to more frequently solicit architectural services.

The College will issue a public solicitation of architectural services to competitively select a service provider to evidence that such services are obtained at the lowest price consistent with desired quality.

Finding No. 4: Improvements were needed in College access controls to ensure that information technology (IT) access privileges were appropriately assigned.

The College is developing system reports by functional manager that will list all users and their system access. The College will distribute these reports to the functional managers who will then: review each user's access level; report that the review has been completed; and identify any security access adjustments to be made. As a further control, an additional report will be generated that shows which functional managers have not completed these required security access reviews.

Finding No. 5: The IT access privileges of some former College employees were not timely deactivated.

The College is reviewing and improving processes to ensure timely deactivation of access privileges of former employees to comply with our Information Security Procedures.

Finding No. 6: Contrary to the requirements of the State of Florida General Records Schedule, the College did not retain some IT access control records.

Previously, the College deleted network access for separated employees to decrease the risk that access privileges could be misused by former employees or others. The College now *deactivates* a separated employee's network account and will not delete the deactivated account for at least one year to be in compliance with the State of Florida General Records Schedule.

Finding No. 7: The College did not have a written IT security incident response plan.

As noted by the Auditor, the College is collaborating on a best practices information security framework developed by International Business Machines under contract with the Florida College System composed of all 28 Florida Colleges, including the College of Central Florida and the College Center for Library Automation. This framework will be used as a basis for strengthening our written security incident response procedures.

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Nevertheless, the College takes IT security incidents very seriously and will develop and implement a written security incident response plan by June 30, 2013 while effort continues on the aforementioned Florida College System information security framework.

Finding No. 8: College IT security controls related to user authentication, data loss prevention, and logging needed improvement.

The College will take appropriate action that it deems necessary to address the auditor recommendations.

Sincerely,

James D. Henningsen, Ed.D.
President