REPORT NO. 2012-038
DECEMBER 2011

BROWARD COLLEGE

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

BOARD OF TRUSTEES AND PRESIDENT

Members of the Board of Trustees and Presidents who served during the 2010-11 fiscal year are listed below:

Sean C. Guerin, Chair
Sean C. Alveshire, Vice Chair
John A. Benz from 8-17-10 (1)
Georgette Sosa Douglass to 7-26-10 (2)
Paul C. Tanner to 4-26-11 (3)
Elizabeth Tonkin from 5-31-11 (4)

J. David Armstrong, Jr., President

Notes: (1) Position vacant from July 1, 2010, to August 16, 2010.
(2) Board member served beyond the end of term, May 31, 2010.
(3) Position vacant from April 27, 2011.
(4) Position vacant from July 27, 2010, to May 30, 2011.

The audit team leader was Enrique A. Alonso, CPA, and the audit was supervised by Ida Marie Westbrook, CPA. For the information technology portion of this audit, the audit team leader was Stephanie J. Hogg, 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.

BROWARD COLLEGE

SUMMARY

Our operational audit disclosed the following:

BOARD POLICIES

Finding No. 1: The College had not implemented an identity theft prevention program contrary to Section 114 of the Fair and Accurate Credit Transaction Act of 2003.

Finding No. 2: The Board had not adopted written policies and procedures relating to electronic funds transfers.

STUDENT TUITION AND FEES

Finding No. 3: The College needed to strengthen its procedures for assessing user fees.

RECEIVABLES

Finding No. 4: The College needed to enhance its procedures related to the billing and collection of student receivables.

PURCHASING

Finding No. 5: The College's monitoring of procurement card credit limits needed improvement.

INFORMATION TECHNOLOGY

Finding No. 6: Some inappropriate or unnecessary information technology (IT) access privileges existed.

Finding No. 7: The College did not timely remove the IT access privileges of some former employees.

Finding No. 8: The College's IT security controls related to user authentication and data loss prevention needed improvement.

BACKGROUND

Broward College (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 five 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 campuses in Coconut Creek, Davie, and Pembroke Pines, and centers located in Dania Beach, Fort Lauderdale, Miramar, Pembroke Pines, and Weston, Florida. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Broward County. The College reported enrollment of 30,470 full-time equivalent students for the 2010-11 fiscal year.

The results of our financial audit of the College for the fiscal year ended June 30, 2011, 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, 2011, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Board Policies

Finding No. 1: Identity Theft Prevention Program

In response to increasingly pervasive risks associated with the custodianship of sensitive information, Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (Act) expanded on the Federal Trade Commission's (FTC) Fair Credit Reporting Act of 1970 to provide clear guidance to businesses and other organizations that process certain personal information that places them at high risk for identity theft. The Act was implemented by the Red Flags Rule (Rule), which went into effect November 1, 2008, and enforcement of the Rule began on January 1, 2011. The Rule requires financial institutions and creditors that hold consumer accounts designed to permit multiple payments or transactions or any other account for which there is a reasonable foreseeable risk of identity theft to develop and implement an identity theft prevention program (Program) for new and existing covered accounts. The Rule requires the College Board to approve the initial written Program. The Program should be designed to detect, prevent, and mitigate identity theft through the identification of warning signs, or "red flags" in day-to-day operations. The Program must be appropriate for the College's size and complexity and the nature and scope of its operations and must contain reasonable policies and procedures to: (1) identify relevant patterns, practices, and specific forms of activity, the red flags, that signal possible identity theft for the covered accounts; (2) detect red flags; (3) respond appropriately to any red flags detected to prevent and mitigate identity theft; and (4) ensure the Program is updated periodically to reflect changes in risks for identity theft.

As a result of its student lending activity, the College meets the definition of a creditor as defined by the FTC and, as such, must comply with the Rule. Subsequent to audit inquiry, the Board approved College Board Policy 6Hx2-6.42 and Procedure A6Hx2-6.42 Identity Theft Prevention Program (ITPP) during its May 24, 2011, meeting. The ITPP contains requirements of the Rule, including, Section VIII (B) of the ITPP, which provides for the training of College personnel. As of June 30, 2011, the College had not provided the required training to College personnel.

The College contracted with a firm to provide training to applicable employees and the College indicated that training is expected to start in October 2011.

Recommendation: The College should continue its efforts to provide training to employees as required by the Red Flags Rule.

Finding No. 2: 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 any funds under their control are allowed to be moved by electronic transaction for any purpose including direct deposit, wire transfer, withdrawal, investment, or payment.

According to the College's records, approximately $24.5 million of electronic funds transfers were made during the 2010-11 fiscal year. In response to our inquiry, College personnel stated that they did not have written policies and procedures related to electronic funds transfers. While the College had established controls over electronic funds transfers, the lack of specific guidance in the form of written policies and procedures increases the risk of misappropriation of funds occurring without timely detection.

Recommendation: **The Board should adopt written policies and procedures related to electronic funds transfers.**

Student Tuition and Fees

Finding No. 3: User Fees

Section 1009.23(12), Florida Statutes, authorizes, each college board of trustees to establish user fees, including laboratory fees, that are not to exceed the cost of the services provided and may only be charged to persons receiving the service. Additionally, the Florida College System Council of Business Affairs and the Florida Department of Education, Division of Florida Colleges, issued guidelines for assessing user fees. These guidelines provide that each college board establish policies for the implementation and justification of additional user fees, defining which costs are in excess of base instructional costs, describing the documentation required to support the fees, the time period for review of such fees, and the manner of presenting such fees to the board for approval. The College Board approved a comprehensive Course Laboratory Fees policy on September 28, 2010, and revised the policy on May 24, 2011. The College recorded laboratory and user fee collections of $4.7 million for the 2010-11 fiscal year.

Our review of laboratory and other user fees in March 2011 disclosed that 268 of the 703 user fees had not been evaluated for appropriateness and compliance with the above-noted guidelines, contrary to the Board's policy, and 693 had not been submitted to the Board for approval contrary to Florida Statutes. College personnel indicated that they were continuing their efforts to evaluate the remaining user fees and obtain Board approval for these fees and, as of July 26, 2011, 129 user fees remained to be evaluated and 491 user fees needed to be submitted for Board approval. A similar finding was noted in our report No. 2010-097.

Recommendation: **The College should ensure that a documented evaluation of each user fee is performed in accordance with the Board's policy, and that all fees are approved by the Board in accordance with Florida Statutes.**

Receivables

Finding No. 4: Student Receivables – Collection Procedures

College Policy 6Hx2-6.16 and corresponding Procedure A6Hx2-6.16 provide that all receivables will be invoiced immediately, a second notice will be sent in 30 days, and a final notice will be sent in 60 days after the first invoice and will include a warning that the College may use a collection agency during the next phase of the collection procedures. If no payment arrangement has been made within 90 days of the due date, the account will be reported to the credit bureau and referred to a collection agency. In addition, for student receivables, a hold is placed on the student's college records for delinquent student accounts. When a student's account is sent to a collection agency there is also a hold placed on registration to prevent them from incurring additional debt to the College. These policies also provide that uncollected accounts older than two years shall be submitted to the Board of Trustees for write-off in accordance with State law.

As of June 30, 2011, College records indicated that receivables related to fee deficiencies totaled $1,962,702. Fee deficiencies are incurred when a student's financial aid award is reduced due to a dropped class or change in financial aid eligibility. The College wrote-off $233,719 of fee deficiencies on May 3, 2011, pursuant to Board approval on

April 26, 2011. Our review of the College's collection procedures related to these fee deficiencies disclosed the following:

- Of 4,349 students with outstanding fee deficiencies, 266 had deficiencies for two or more terms totaling $298,000. The College's policies do not restrict students from registering for classes in a subsequent term until their accounts are referred to a collection agency or approximately 90 days after the receivable has been established. Placing a hold on a student's registration when amounts become due would enhance the College's ability to collect amounts due from students.
- Billing statements sent to students did not accurately reflect the full amount due to the College. Whenever there is an increase in the amount due to the College for a fee deficiency, the statement sent to the student indicates the total amount owed under a column titled "original amount;" however, only the increase in amounts due is shown in the "balance due" column and at the top of the statement. The final notice that is sent to warn the student that the account will be sent to collection does reflect the correct total amount due to the College. In response to our inquiry, the College indicated that the billing is an automated process and they are currently working on implementing a new billing system to correct the error in amounts invoiced to the student. Inaccurate billing can lead to disputes regarding the amounts due to the College and increases the risk that a receivable may become uncollectible.

Recommendation: The College should enhance collection procedures to restrict a student from registering for classes if they have any outstanding balance and ensure that billing statements are accurate as to the total amount owed.

Purchasing

Finding No. 5: Procurement Cards

The College administers a procurement card (P-card) program, by which it authorizes the issuance of credit cards to employees to purchase certain work-related goods and services. The primary objective of the program is to expedite the ordering, receiving, and payment processes without the use of the standard requisition and purchase order system by delegating limited purchasing authority to the cardholders. The College issued procurement cards to 290 employees as of June 30, 2011, and incurred charges totaling approximately $1.3 million during the 2010-11 fiscal year.

The College's Procurement Card Program Procedures manual designates each department head as being responsible for approving P-card applications and any changes in credit limits. Our review of cardholder monthly credit limits for 20 employees from July 2010 through June 2011 disclosed 6 employees with monthly credit limits that appeared excessive based on the employee's actual P-card use, as shown in the table below:

Employee Title	Monthly Limit	High
Bursar (1)	$10,000.00	$127.20
Journeyman, HVAC Technician (2)	5,000.00	687.84
Journeyman, HVAC Technician (2)	5,000.00	900.07
District Director, Enrollment Manager (3)	2,500.00	273.55
Interim Associate Dean (3)	2,500.00	643.25
Interim Associate Dean	1,500.00	381.67

Notes: (1) Back-up for parking permits.
(2) For emergency use.
(3) Cards less than one year old.

In addition, we noted 18 other P-cardholders that had no charges in the 2010-11 fiscal year. Establishing effective controls to monitor the reasonableness of P-card monthly credit limits reduces the risk of unauthorized use. Subsequent to audit inquiry, College personnel closed 4 of the cardholder's accounts.

Recommendation: The College should periodically evaluate authorized P-card limits and usage by cardholders to determine the need for the cards issued and establish appropriate spending limits.

Information Technology

Finding No. 6: 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 outside of their areas of responsibility. Periodically reviewing IT access privileges assigned to employees promotes good internal control and is necessary to ensure that employees cannot access computer resources inconsistent with their assigned job responsibilities.

Our test of selected access privileges to the finance and human resources applications disclosed that some security groups and employees had access privileges that either permitted the employees to perform incompatible duties or were not necessary for their job duties. Specifically:

- Access privileges assigned to one security group included the ability to, among other things, create and maintain invoices; create on-demand payments; and maintain payables, credit memos, banking information, and employee deductions, contrary to an appropriate separation of duties. All employees who were members of this group inherited these access privileges that were unnecessary for the employees' job duties.
- Access privileges assigned to another security group included the ability to, among other things, maintain student term advisement information and update utility code tables. All employees who were members of this group inherited these access privileges that were unnecessary for the employees' job duties.
- Access privileges assigned to another security group included the ability to, among other things, maintain finance overrides and maintain personnel system profiles, contrary to an appropriate separation of duties. All employees who were members of this group inherited these access privileges that were unnecessary for the employees' job duties.
- One IT employee had the ability to, among other things, perform security module maintenance, maintain security systems, and perform functions related to job scheduling. This combination of access privileges was unnecessary for the employee's job duties and contrary to an appropriate separation of duties.
- One business adjunct instructor had the ability to, among other things, perform employee maintenance of employee demographic information. Employee maintenance privileges were unnecessary for the employee's job duties and contrary to an appropriate separation of duties.
- Nineteen employees from various departments had the ability to, among other things, maintain personnel system profiles, update and delete selected tables, update and purge e-mail messages, update batch submissions, and update user defaults. These security group privileges were unnecessary for the employees' job duties and contrary to an appropriate separation of duties.

Although end-user departments performed annual access reviews, the existence of the incompatible or unnecessary access privileges indicated a need for improved College review of access privileges. Without a comprehensive review, inappropriate access privileges may not be timely detected and addressed by the College, increasing the risk of unauthorized disclosure, modification, or destruction of College data and IT resources.

Recommendation: The College should enhance its process of reviewing the appropriateness of IT application access privileges, including those granted within a security group, and timely remove or adjust any inappropriate or unnecessary access detected to ensure that access privileges are compatible with employee job duties.

Finding No. 7: Timely Removal of Access Controls

Effective management of system access privileges includes the timely removal of employee IT access privileges when employment is terminated. Prompt action is necessary to ensure that the access privileges are not misused by former employees or others.

Our test of 70 former employees who terminated employment from the College during the period July 1, 2010, through January 31, 2011, disclosed that 18 did not have their access privileges to the College's computer systems removed in a timely manner, 12 of which had access to data systems. The access privileges of the 18 former employees remained active from 3 to 105 days after the employees' termination date. In response to audit inquiry, College personnel stated that the College's system deletes terminated employees from accessing the system as of the date of the employee's termination based on termination dates entered into the system by Human Resources Department personnel; however, personnel within each College department are responsible for submitting the termination date to Human Resources Department personnel, and delays in the Human Resources Department receiving the information hinder the timely termination of the access privileges.

Although the computer data file and system access privileges had been removed for all former employees included in our test, failure to timely remove such access increases the risk that access privileges could be misused by former employees and others. A similar finding was noted in our report No. 2010-097.

Recommendation: The College should continue its efforts to implement a process to ensure the timely removal of access privileges of former employees.

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

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that certain College security controls related to user authentication and data loss prevention 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 and data loss prevention, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that College data and IT resources may be subject to improper disclosure, modification, or destruction.

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

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the College had taken corrective actions for findings included in our report No. 2010-097.

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 January 2011 to July 2011 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: (1) obtain an understanding and make overall judgments as to whether College internal controls promoted and encouraged compliance with applicable laws, rules, regulations, contracts, and grant agreements; the economic and efficient operation of the College; the reliability of records and reports; and the safeguarding of assets; (2) evaluate management's performance in these areas; and (3) determine whether the College had taken corrective actions for findings included in our report No. 2010-097. Also, pursuant to Section 11.45(7)(h), Florida Statutes, our audit may identify statutory and fiscal changes to be recommended to the Legislature.

The scope of this operational audit is described in Exhibit A. Our audit included examinations of various records and transactions (as well as events and conditions) occurring during the 2010-11 fiscal year.

Our audit methodology included obtaining an understanding of the internal controls by interviewing College personnel and, as appropriate, performing a walk-through of relevant internal controls through observation and examination of supporting documentation and records. Additional audit procedures applied, to determine that internal controls were working as designed, and to determine the College's compliance with the above-noted audit objectives, are described in Exhibit A. Specific information describing the work conducted to address the audit objectives is also included in the individual findings.

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 access controls and user authorization.	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, network, and applications to determine the appropriateness based on the employees' job functions and responsibilities and adequacy with regard to preventing the performance of incompatible duties.
Procedures to timely prohibit former employees' access to electronic data files.	Tested access privileges to data files for employees who terminated employment during the audit period and verified that the College terminated access privileges.
IT security controls, user authentication, and data loss prevention.	Reviewed written policies, procedures, and programs in effect governing the classification, management, and protection of sensitive and confidential information, security controls, and user authentication.
IT security incident response.	Reviewed written policies and procedures, plans, and forms related to security incident response and reporting.
IT risk management and assessment.	Reviewed the College's risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.
Fraud policy and related procedures.	Examined written policies, procedures, and supporting documentation 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 receivables.	Tested student receivables to determine whether the receivable was properly authorized, documented, and within established limits. Determined adequacy of collection and write-off procedures, and whether accounts written-off were properly approved.
Florida residency determination and tuition.	Tested student registrations to determine whether the College documented Florida residency and correctly assessed tuition in compliance with Section 1009.21, Florida Statutes, and State Board of Education Rule 6A-10.044, Florida Administrative Code.
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.

EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Procedures for assessing, calculating, collecting, cancelling, recording, and supporting student fees.	Tested student fees to verify the authority for student fees assessed; the accuracy of calculations of fees assessed; the proper collection of late fees, if appropriate; the issuance of a receipt; and the deposit of collections to the central cashier's records. Also, tested to verify that registration was cancelled if the fees were not paid when due, that student status and residency were supported, and that deferred fees were recorded as a receivable.
Laboratory and user fees.	Reviewed the College's procedures and determined whether they were approved by the Board of Trustees. Tested laboratory and user fees and examined supporting documentation to determine whether the College properly calculated these fees.
Overtime payments.	Reviewed College policies, procedures, and supporting documentation evidencing the approval of and necessity for overtime payments.
Contractual agreements.	Determined whether contractual services were supported by Board-approved contracts. Also, examined and tested the aforementioned contracts to ensure that they were properly awarded and executed, that contract terms were adequately supported, and that vendors carried adequate insurance.
Construction administration.	For selected major construction projects, tested payments and supporting documentation to determine compliance with College policies and procedures and provisions of law and rules. Also, for construction management contracts, determined whether the College monitored the selection process of subcontractors by the construction manager.
Procedures for 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 recent construction projects to determine whether architects and engineers provided evidence of the required insurance.
Annual fire safety, casualty safety, and sanitation inspection reports.	Obtained copies of the most recent annual fire safety, casualty safety, and sanitation inspection reports and determined whether deficiencies noted were timely corrected.
Wireless communication devices.	Reviewed policies and procedures to determine whether the College limited the use of, and documented the level of service for, wireless communication devices.
Electronic payments.	Reviewed College policies and procedures relating to electronic payments and tested supporting documentation to determine if selected electronic payments were properly authorized and supported.
Self-insurance for employee health.	Reviewed College procedures to inform the third-party administrator of the eligibility of employees and dependents. Tested claims processed by third-party administrator.
Severance pay limitations.	Determined whether any new or renewed employment contracts entered into on or after July 1, 2011, included any type of bonus or severance pay.

EXHIBIT B
MANAGEMENT'S RESPONSE

BROWARD COLLEGE
www.broward.edu

OFFICE OF THE CONTROLLER
Willis Holcombe Center
Phone 954-201-7435/Fax 954-201-7309

WILLIS HOLCOMBE CENTER
111 East Las Olas Blvd.
Fort Lauderdale, FL 33301

INSTITUTE FOR ECONOMIC DEVELOPMENT
111 East Las Olas Blvd.
Fort Lauderdale, FL 33301

A. HUGH ADAMS CENTRAL CAMPUS
3501 S.W. Davie Road
Davie, FL 33314

NORTH CAMPUS
1000 Coconut Creek Blvd.
Coconut Creek, FL 33066

JUDSON A. SAMUELS SOUTH CAMPUS
7200 Hollywood/Pines Blvd.
Pembroke Pines, FL 33024

PINES CENTER
16957 Sheridan St.
Pembroke Pines, FL 33331

WESTON CENTER
4205 Bonaventure Blvd.
Weston, FL 33332

MIRAMAR AUTOMOTIVE/ MARINE CENTER
7451 Riviera Blvd.
Miramar, FL 33023

MIRAMAR TOWN CENTER
2050 Civic Center Place
Miramar, FL 33025

TIGERTAIL LAKE RECREATIONAL CENTER
580 Gulfstream Way
Dania Beach, FL 33004

December 2, 2011

The Florida Auditor General
Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399

Dear Sir/Madam:

Attached herewith, please find the responses to Broward College's Operational Audit Preliminary and Tentative Findings for the fiscal year ended June 30, 2011.

Finding No. 1: Identity Theft Prevention Program
Acknowledged. Broward College provided College-wide staff training November 1st through November 4th, 2011. Training was provided to approximately 50 department heads and administrators. Upon completion of the training sessions, department heads were able to train their staff and create protocols for their departments to detect, prevent, and respond to patterns that may indicate identity theft. Additionally, a twelve member Identity Theft Prevention Team was appointed and provided with the necessary knowledge of compliance issues and best practices to further refine, review, and improve the College's Identity Theft Prevention Program.

Finding No. 2: Electronic Funds Transfer
Acknowledged. On October 25, 2011 the Board adopted, Policy and Procedure 6Hx2-6.40 related to electronic funds transfers.

Finding No. 3: User Fees
Acknowledged. At the September 27th, 2011 Board meeting the college presented and received approval for the balance of outstanding user fees which had been reviewed and evaluated by the college for appropriateness and compliance with Florida Statute. The college has in place a newly developed process to regularly assess user fees.

Finding No. 4: Student Receivables – Collection Procedures
Acknowledged. Effective October 18, 2011, the College began placing an immediate registration hold on student accounts for specific debt types. This measure now requires students to satisfy existing debt before being permitted to enroll in additional classes for either the current or future semesters.
Effective July 11, 2011 student bills and dunning letters now accurately reflect the total debt due to the College.

Finding No. 5: Procurement Cards
Acknowledged. The College will implement an annual review of cardholder activity to determine appropriate p-card limits based on past activity. However, for certain positions, such as those responsible for maintenance and emergency response areas, it is not prudent to reduce p-card limits based on an annual usage history alone as these cardholders may require the available spending authority should an emergency arise.

Finding No 6: Access Privileges
Acknowledged. In collaboration with functional business units, Information Technology will enhance the process of administering application access using information security best practices, including documented procedures and controls. This is currently in progress and should be completed by April 30th, 2012.

Finding No 7: Timely Removal of Access Controls
Acknowledged. Information Technology in collaboration with Human Resources will develop an automated solution to improve the current process to ensure the timely removal of access privileges of former employees. This is currently in progress and should be completed by June 30th , 2012.

Finding No 8: Security Controls-User Authentication and Data Loss Prevention
Acknowledged. Information Technology will implement recommendations regarding password policy by February 28th, 2012. Data Loss Prevention Program policy changes will be approved and implemented by March 30th, 2012.

Yours truly,
Jayson Iroff
Jayson Iroff
Controller