REPORT NO. 2012-068
JANUARY 2012

PENSACOLA STATE 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:

	County
John L. O'Connor, Chair	Santa Rosa
Edward Moore, Jr., Vice Chair (1)	Escambia
Carol H. Carlan	Escambia
Monsignor Luke Hunt (1)	Santa Rosa
Margie T. Moore (1)	Escambia
Paul R. Snider (2)	Santa Rosa
Dona W. Usry (2)	Escambia
Herbert R. Woll	Santa Rosa
Deidre L. Young (2)	Escambia

Dr. Charles E. Meadows, President

Notes: (1) Board member served beyond the end of term, May 31, 2011.
(2) Board member served beyond the end of term, May 31, 2010.

The audit team leader was Joseph D. Dykes, CPA, and the audit was supervised by James W. Kiedinger, Jr., 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.

PENSACOLA STATE COLLEGE

SUMMARY

Our operational audit disclosed the following:

BOARD POLICIES

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

PURCHASING

Finding No. 2: The College needed to enhance its purchasing card controls.

STUDENT FEES AND ENROLLMENT

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

Finding No. 4: The College needed to strengthen its controls to ensure the accurate reporting of instructional contact hours for adult general education classes to the Florida Department of Education.

INFORMATION TECHNOLOGY

Finding No. 5: Some inappropriate or unnecessary information technology (IT) access privileges existed.

Finding No. 6: The College's IT security controls related to user authentication needed improvement.

BACKGROUND

Pensacola State 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 nine 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 Pensacola, Milton, and Warrington, Florida. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Escambia and Santa Rosa Counties. The College reported enrollment of 9,336 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. The Board approved Board Policy 6Hx20-1.037 on April 21, 2009, which requires that the President or his designee prepare a written Program; however, as of June 30, 2011, the Board had not approved a written Program. Additionally, training required by the Rule had not been provided to employees who have access to accounts or personally identifiable information that may constitute a risk to the College or its students. In these circumstances, the College or its students could be at increased risk of identity theft due to the sensitive nature of information that is obtained, held, and processed through the student lending process. In addition, noncompliance with the Rule could result in monetary penalties from the FTC. College personnel indicated that lack of compliance with the Rule was largely a result of confusion as to the applicability of the Rule to colleges.

Recommendation: The College should continue its efforts to implement an identity theft prevention program as required by the Red Flags Rule.

Purchasing

Finding No. 2: Purchasing Cards (P-card)

The College administers a P-card program, which gives employees the convenience of purchasing items without using the standard purchase order process. The College uses P-cards to expedite low dollar purchases of goods and services. P-cards are subject to the same rules and regulations that apply to regular College purchases, and the College has established P-card procedures to provide users with additional guidance on how to properly use the P-cards. College procedures require that appropriate College departments prepare monthly P-card activity logs to facilitate the reconciliation between P-card bank data and College records and to document approval of non-travel[1] P-card activity for the respective departments. The College issued P-cards to 105 employees and incurred charges totaling approximately $390,000 during the 2010-11 fiscal year.

Our review of 43 P-card transactions, totaling $14,607, disclosed that the College's controls over the P-card program needed improvement, as follows:

- College personnel did not include 22 transactions, totaling $3,932, on monthly P-card activity logs. Accordingly, Department-level reconciliations of these transactions to P-card bank data were not documented.

[1] Travel authorization forms are approved by supervisory personnel prior to travel expenses being charged to purchasing cards.

- Although P-card activity logs were prepared for 7 transactions totaling $1,244, the supervisors did not indicate approval of the transactions by signing the logs. For these 7 transactions and the 22 transactions discussed above, totaling $5,176, there was no evidence of supervisory approval of the transactions.
- As a result of not maintaining detailed receipts for 6 transactions totaling $617, the College did not document that the charges were for an authorized public purpose and in accordance with the College's P-card policies and procedures. Subsequent to our bringing these transactions to their attention, College personnel obtained receipts and created activity logs for the transactions.
- For 6 transactions, totaling $1,187, for food items for the Board, aromatherapy gift sets, movie tickets, shirts, and a gift card, College records did not document how these purchases served a public purpose. College employees used College P-cards to make these purchases on behalf of other College-affiliated organizations (including the Foundation). Subsequent to our inquiry, two of the purchases, totaling $175, were reimbursed from agency accounts and the Pensacola State College Foundation, Inc., reimbursed the remaining four purchases, totaling $1,012.
- Three transactions included payment of State sales tax totaling $52, although Section 212.08(7)(o), Florida Statutes, exempts the College from paying State sales tax.

In the above instances, College personnel did not follow established College procedures, increasing the risk of unauthorized charges without timely detection.

Recommendation: The College should enhance its P-card controls to ensure compliance with established College procedures.

Student Fees and Enrollment

Finding No. 3: Student User Fees

Section 1009.23(12), Florida Statutes, authorizes the Board of Trustees (Board) to establish user fees, including laboratory fees, that shall not exceed the cost of the services provided and can only be charged to persons receiving the service. State Board of Education Rule 6A-14.054(6), Florida Administrative Code, authorizes the Board to establish user fees in addition to tuition fees for services that incur unusual costs. Additionally, the Florida College System Council of Business Affairs and the Florida Department of Education (FDOE), Division of Florida Colleges, have issued guidelines for assessing user fees. These guidelines provide that the 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.

During the 2010-11 fiscal year, the College collected $834,000 from laboratory and other user fees assessed on approximately 250 courses with laboratory fees ranging from $10 to $387 a course. College procedures for assessing laboratory and other user fees needed improvement, as follows:

- The College's Board Policy 6Hx20-3.019 provided for the establishment of laboratory and user fees for individual courses; the manner of presenting such fees to the Board for approval; and inclusion of the procedure for justification, determination of excess costs, and review in the Administrative Procedures Manual (Manual). However, the College had not established procedures providing guidance that defined base instructional costs, described documentation required to support the fees, or identified the time period for review of such fees. Consequently, College records did not demonstrate for any courses that the costs described in supporting documentation for laboratory and other user fees assessed did not exceed the course's base instructional cost.

- Our review of 12 courses for which laboratory or other user fees were assessed during the 2010-11 fiscal year disclosed that for 5 of the courses, College records described items covered in the laboratory fee, but did not document the reasonableness of the item costs. For example, the College charged a $175 laboratory fee for a dental clinic course and received $5,600 in laboratory fees for this course during the 2010-11 fiscal year. Supporting documentation for $75 of the laboratory fee included disposable items such as antibacterial hand wash, sterilization pouches, soft picks, interdental picks, sterile wrap, dental floss, disposable mouth mirrors, rubber tip stimulators, floss threaders, etc. However, the College did not quantify these items or otherwise provide unit costs to support that estimated costs included in the documentation were reasonable. Absent such information, the College's records did not demonstrate that the fees assessed were properly calculated and did not exceed the costs of services provided.

In the absence of written procedures, including established guidelines for determining base instructional costs, laboratory and other user fees may not be properly calculated and may exceed the costs incurred to provide the services.

Recommendation: The College should develop and implement written procedures for laboratory and other user fees to ensure compliance with Section 1009.23(12), Florida Statutes, and the guidelines provided by the Florida College System Council of Business Affairs and FDOE, Division of Florida Colleges, and such procedures should be submitted to the Board for review and approval.

Finding No. 4: Adult General Education

Section 1004.02(3), Florida Statutes, defines adult general education, in part, as comprehensive instructional programs designed to improve the employability of the State's workforce. The College received State funding for adult general education, and proviso language included in Chapter 2010-152, Laws of Florida, Specific Appropriation 112, required that each college report enrollment for adult general education programs identified in Section 1004.02, Florida Statutes, in accordance with the Florida Department of Education (FDOE) instructional hours reporting procedures.

Procedures provided by FDOE stated that fundable instructional contact hours are those scheduled hours that occur between the date of enrollment in a class and the withdrawal date or end-of-class date, whichever is sooner. Additionally, there is a minimum enrollment threshold of 12 hours of attendance per program that must be met before a student can be counted for funding purposes; however, when the threshold is not met the actual hours of attendance should still be included to satisfy other reporting requirements.

The College reported 489,838 instructional hours for adult general education classes provided to students during the 2010-11 fiscal year. Our test of 30 students, enrolled in 57 adult general education classes, for which the College reported 3,851 hours to FDOE during the 2010-11 fiscal year, disclosed errors in reporting instructional contact hours for 13 of the 30 students tested, as follows:

- For 7 students, we identified nine separate instances in which the College did not track actual attendance because the instructors did not maintain student sign-in sheets or attendance records. Therefore, College records did not evidence that the 12-hour threshold had been met or what number of hours should have been reported. The College reported 634 hours for these students.
- For 6 students, the calculated instructional hours based on verified dates of student attendance did not agree with instructional hours reported to FDOE because College personnel recorded the wrong dates of student attendance. As a result of these errors, the College over reported enrollment by 125 hours for 5 students and under reported enrollment by 17 hours for 1 student enrolled in adult general education classes during the 2010-11 fiscal year.

Since future funding may be based, in part, on enrollment data submitted to FDOE, it is important that the College submit accurate data.

Recommendation: The College should strengthen its controls to ensure accurate reporting of instructional contact hours for adult general education classes to FDOE. The College should also contact FDOE to determine what corrective actions are necessary regarding the over- and under-reported hours.

Information Technology

Finding No. 5: 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.

In the College's finance and human resource applications, employees were assigned to roles that represented groupings of access privileges. Our audit test of selected access privileges to the finance and human resources applications disclosed that some application roles had access privileges that permitted the employees to perform incompatible duties. Specifically:

- Access privileges assigned to one finance application role included the ability to reset passwords and update user profiles. Although Information Technology Services (ITS) employees having responsibilities related to security required the privileges, all employees who were assigned the role inherited the ability to reset passwords and update user profiles. In response to our inquiry, College management removed these access privileges from this role.
- ITS employees were assigned to a finance application role that included access privileges providing the ability to reset passwords; update user profiles; add, update, or remove roles, activities, and security levels; update vendor information; approve or deny requisitions; create, update, and approve journal entries; start the check proof and print process; and add or change salary records. Allowing ITS employees all of the access privileges within this role was unnecessary for their assigned job responsibilities and contrary to an appropriate separation of duties. In addition, two ITS employees who no longer had security responsibilities were assigned this role. In response to our inquiry, College management removed these access privileges and the two ITS employees from this role.
- Access privileges assigned to one human resources application role included the ability to clear a pay control field, allowing changes such as pay rate updates to take effect. ITS employees were assigned to this role and thereby inherited the access privilege for clearing a pay control field that was unnecessary for their job responsibilities and contrary to an appropriate separation of duties. In response to our inquiry, College management removed this access privilege from the role.

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 or unnecessary 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 for reviewing the appropriateness of application access privileges, including those granted within application roles, and timely remove or adjust any inappropriate or unnecessary access detected to ensure that access privileges are compatible with employee job duties.

Finding No. 6: Security Controls – User Authentication

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 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, 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 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. 2010-023.

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 January 2011 to September 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. 2010-023. 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 network and administration 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 network and applications to determine the appropriateness and necessity based on the employees' job functions and responsibilities and adequacy with regard to preventing the performance of incompatible duties.
IT termination of employee access.	Reviewed procedures to remove former employees' access to electronic data files. Tested access privileges of former employees to determine whether their access privileges had been timely removed.
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.	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.
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.
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.
Overtime payments.	Analytical procedures determined that overtime payments were insignificant.
Laboratory and other 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.
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
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.
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 related to electronic payments and if significant, tested supporting documentation to determine if selected electronic payments were properly authorized and supported.
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.

EXHIBIT B
MANAGEMENT'S RESPONSE

PENSACOLA STATE COLLEGE
Office of the President

January 3, 2012

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

Dear Mr. Martin:

In response to your letter dated December 1, 2011 containing the "preliminary and tentative audit findings and recommendations," I offer the following:

Finding No. 1: Identity Theft Prevention Program.
The college has prepared procedures that will be reviewed and approved by the President's Council.

Finding No. 2: Purchasing Cards.
The College has implemented additional training for all employees that have been issued purchasing cards to ensure that they are following the rules established by the college for purchasing card transactions.

Finding No. 3: Student User Fees.
The college is working to establish the procedures recommended in the audit finding and will have those in place for the Summer 2012 semester.

Finding No. 4: Adult General Education.
The college will continue to work with the instructors to ensure the accurate reporting of enrollment for these students.

Finding No. 5: Access Privileges.
The college made changes as indicated in the audit finding.

Finding No. 6: Security Controls – User Authentication.
The college has taken action to correct the specific issues.

Please accept my sincere appreciation for another positive audit process.

Sincerely,

Edward Meadows
President