

# SOUTH FLORIDA COMMUNITY COLLEGE

---

## Operational Audit



## BOARD OF TRUSTEES AND PRESIDENT

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

	<u>County</u>
Gary Delatorre, Vice Chair to 7-27-10, Chair from 7-28-10 (1)	Hardee
Timothy D. Backer, Vice Chair from 7-28-10	DeSoto
George David Leidel, Jr., Chair to 7-27-10 (2)	Highlands
Tamela "Tami" C. Cullens (1)	Highlands
Joan H. Hartt (1)	Highlands
Dr. Louis H. Kirschner	DeSoto
Richard L. Maenpaa (2)	Hardee
Anne D. Reynolds (2)	Highlands

Dr. Norman L. Stephens, Jr., President

- Notes: (1) Board member term expired on May 31, 2010, and  
Board member continued to serve through June 30, 2011.  
(2) Board member term expired on May 31, 2011, and  
Board member continued to serve through June 30, 2011.

The audit team leader was Gregory J. Lemieux, CPA, and the audit was supervised by David A. Blanton, CPA. For the information technology portion of this audit, the audit team leader was Rebecca Ferrell, 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](mailto: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](http://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.

**SOUTH FLORIDA COMMUNITY COLLEGE**

**SUMMARY**

**Our operational audit disclosed the following:**

**EXPENSES AND DISBURSEMENTS**

**Finding No. 1:** College records did not evidence the authorized public purpose of certain travel expenses associated with an annual conference.

**INFORMATION TECHNOLOGY**

**Finding No. 2:** Some inappropriate or unnecessary information technology (IT) access privileges existed.

**Finding No. 3:** The College had not developed a written, comprehensive IT risk assessment.

**Finding No. 4:** The College’s IT security controls related to user authentication needed improvement.

**BACKGROUND**

South Florida Community 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 eight 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 Avon Park, Lake Placid, Bowling Green, and Arcadia, Florida. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Highlands, Hardee, and DeSoto Counties. The College reported enrollment of 2,737 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**

**Expenses and Disbursements**

**Finding No. 1: Travel Expenses**

Section 112.061, Florida Statutes, governs travel expenses of officers, employees, and authorized persons traveling on behalf of public agencies, including State colleges. The College reported travel expenses totaling \$337,009 for the 2010-11 fiscal year.

Our test of 27 travel expenses totaling \$28,372 disclosed that the College paid for conference registration fees and other travel expenses totaling \$3,793 from the unrestricted current fund for a former Board member, who last served on the College Board 27 years ago (serving between 1976 and 1983), and a College instructor for the purpose of accepting individual awards at the Association of Community College Trustees 2010 Annual Leadership Congress in

Toronto, Canada. However, Attorney General Opinion (AGO) No. 079-105, provides that travel for accepting a personal award does not constitute a valid public purpose. AGO No. 079-105, states an officer's travel expenses may be paid from public funds only when the travel is for a public purpose authorized by law to be performed by the agency or official in question, is necessary for the conduct of official business of the State, and is necessary for the performance of the officer's official duties. AGO No. 079-105 further states that while the receipt of a personal award might be said to have some positive effect on the state in general or the agency with which the officer is connected, the primary benefit would necessarily be a personal and private benefit to the officer and any public benefit would be only incidental; therefore, there could be no instance in which expenses incurred in accepting a personal award could properly be paid for from public funds.

---

**Recommendation:** The College should enhance its procedures to ensure that travel expenses are limited to those that serve an authorized public purpose in conducting official business. In the absence of an authorized public purpose for the \$3,793 of travel expenses, the College should seek to restore this amount to the unrestricted current fund.

---

<b>Information Technology</b>
-------------------------------

---

**Finding No. 2: 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.

Our audit tests of selected access privileges to the finance and human resources (HR) applications, and the supporting operating system and database, disclosed some user accounts with inappropriate or unnecessary access privileges, as follows:

- One application-delivered user account, and one test account utilized in testing software changes, had update access to HR and payroll information. One additional application-delivered user account, utilized for software upgrades, also had update access to HR and payroll information in addition to finance information. The access privileges were unnecessary and inappropriate for the purposes of these accounts. Another application-delivered user account that had been utilized for data conversion but was no longer necessary for operations had database administration access privileges in addition to update access privileges to HR, payroll, and finance information. In response to our inquiry, College management removed these accounts.
- Two application user accounts belonging to IT department staff had the ability to create or modify vendors, enter purchase orders and journal vouchers, process invoices, print checks, define employee positions, add or modify employee information, and enter time and pay adjustments, contrary to an appropriate separation of duties. In response to our inquiry, College management removed these accounts.
- One application-delivered account used for the security administration of the application was shared by three employees, limiting the College's ability to assign responsibility for system actions taken using the account to a specific employee.
- One application-delivered account, used for running application installations, was no longer necessary. In response to our inquiry, College management locked this account.

Although the College performed an annual review of employee access privileges, these inappropriate 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 periodically reviewing the appropriateness of access privileges, including the evaluation of privileges allowed within the application and database, and timely remove or adjust any inappropriate or unnecessary access detected to ensure that access privileges are compatible with employee job duties.

---

---

### Finding No. 3: Risk Assessment

---

Management of IT-related risks is a key part of enterprise IT governance. Incorporating an enterprise perspective into day-to-day governance actions helps an entity understand its greatest security risk exposures and determine whether planned controls are appropriate and adequate to secure IT resources from unauthorized disclosure, modification, or destruction. IT risk assessment, including the identification of risks and the evaluation of the likelihood of threats and the severity of threat impact, helps support management's decisions in establishing cost effective measures to mitigate risk and, where appropriate, formally accept residual risk.

Although the College had informally considered external and internal risks and identified security controls, such as selected configuration settings and policies and procedures, to mitigate these risks, the College had not developed a written, comprehensive IT risk assessment. According to College personnel, the Florida College System (comprised of the 28 Florida Colleges) and the College Center for Library Automation have contracted with a vendor to assist in the development of a best practices information security framework. The completed document, once approved, will include security risk management best practices that the College plans to use to conduct a formal risk analysis. The absence of a written, comprehensive IT risk assessment may limit the College's assurance that all likely threats and vulnerabilities have been identified, the most significant risks have been addressed, and appropriate decisions have been made regarding which risks to accept and which risks to mitigate through security controls.

---

**Recommendation:** The College should develop a written, comprehensive IT risk assessment to provide a documented basis for managing IT-related risks.

---

---

### Finding No. 4: Security Controls – User Authentication

---

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 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. 2010-009.

**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 February 2011 to August 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. 2010-009. 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) 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.	Tested selected access privileges over the database and finance and human resources applications to determine the appropriateness and necessity based on employees’ job duties and user account functions and adequacy with regard to preventing the performance of incompatible duties. Tested administrator account access privileges granted and procedures for oversight of administrator accounts for the network, operating system, database, and application to determine whether these accounts had been appropriately assigned and managed.
IT data loss prevention.	Reviewed the College’s written policies and procedures governing the classification, management, and protection of sensitive and confidential information.
IT security incident response.	Reviewed the College’s written policies and procedures related to security incident response and reporting.
IT risk management and assessment.	Determined whether a written, comprehensive IT risk assessment had been developed.
IT authentication controls.	Reviewed supporting documentation to determine whether authentication controls were configured and enforced in accordance with IT best practices.
Board meetings.	Reviewed Board minutes and, for selected Board meetings, examined supporting documentation evidencing compliance with Sunshine Law requirements (i.e., proper notice of meetings, ready access to public, maintaining of minutes).
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.
Statements of financial interest requirements of Section 112.3145(2), Florida Statutes.	Determined whether the College President and Board members filed statements of financial interest in accordance with law.
Direct-support organizations.	Determined whether audits of direct-support organizations were filed timely with the Auditor General, were done in accordance with generally accepted government auditing standards, and otherwise complied with the applicable Rules of the Auditor General.

**EXHIBIT A (CONTINUED)**  
**AUDIT SCOPE AND METHODOLOGY**

Scope (Topic)	Methodology
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.
Laboratory and other user fees.	Reviewed 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.
Payroll and personnel.	Tested payroll transactions to determine the accuracy of the rate of pay, validity of employment contracts, adequacy of qualifications, completion of performance evaluations, accuracy of leave records, and certifications by supervisory personnel of employee time reports. Also, tested new hires to determine whether personnel records evidenced that employees had the necessary qualifications, degrees, experience, etc.
Background checks.	Tested to determine whether the College had obtained background checks for new hires.
Mandatory and nonmandatory transfers.	Tested transfers made between funds to determine propriety of transfers of restricted moneys between funds.
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 travel expenses to determine whether transactions were adequately supported, and mileage and per diem rates were in accordance with Florida Statutes, and were for College purposes.
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.
Expenditures from non-Federal grants and appropriations.	Determined whether the College received money from non-Federal grants and appropriations, identified the fees collected from these sources, and tested the related expenditures to ensure compliance with grantor restrictions applicable to the specific grants.
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.

**EXHIBIT A (CONTINUED)**  
**AUDIT SCOPE AND METHODOLOGY**

<b>Scope (Topic)</b>	<b>Methodology</b>
Electronic vendor payments.	Reviewed College policies and procedures related to electronic payments and tested supporting documentation to determine if selected electronic payments were properly authorized and supported.
Student enrollment reporting.	Reviewed procedures for student enrollment reporting and verified that FTE reports were supported by student enrollment records and timely transmitted.
Adult general education 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**



December 12, 2011

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

Dear Mr. Martin:

Let me express our sincere appreciation for the professional manner in which your staff conducted the audit. Following are the College's responses to the preliminary and tentative findings to be included in the operational audit report for the fiscal year ended June 30, 2011.

**Finding No. 1 Travel Expenses**

**Recommendation:** The College should enhance its procedures to ensure that travel expenses are limited to those that serve a valid, documented public purpose. In the absence of a documented public purpose for the \$3,793 of travel expenses, the College should seek to restore this amount to the unrestricted current fund.

**Response:** The questioned travel expense did serve a valid public purpose that was documented and approved by the president of the college, the agency head, in accordance with guidance included in AGO No. 79-76 and as required by F.S. 112.061. Nevertheless, the questioned expense of (\$3,793) was restored to the unrestricted current fund as recommended.

The Attorney General Opinion which was cited by the auditors (AGO No. 079-105) pertains to *personal* awards but provides no definition or distinction. These national awards in question recognized two individuals for their exemplary service to South Florida Community College. These awards were professional achievement awards for services directed to, and for the college. These were definitely not *personal* awards for services rendered outside the scope of responsibilities or relationships to the college, past or present.

As stated in AGO No. 79-76 in response to the Auditor General seeking clarification regarding travel, "A determination, however, as to whether travel expenses are incurred in the performance of a duty or function authorized by law to be performed by the university must be made by the head of the university on an individual basis from the peculiar facts and circumstances at the time such activity or such expenditure is authorized or incurred." In accordance with F.S. 112.061, the college president (agency head) authorized and approved the travel in advance, using his official judgment regarding the public purpose and

**EXHIBIT B (CONTINUED)**  
**MANAGEMENT'S RESPONSE**

appropriateness of these travel expenses. Furthermore, the public purpose of the travel was documented and provided to the auditors.

Additionally, the receipt of national awards for services to the college, was not the sole purpose for the travel. Both individuals receiving awards actively participated in professional and board of trustee development programs offered at the conference at which the national awards were announced.

**Finding No. 2 Access Privileges**

**Recommendation:** The College should enhance its process for periodically reviewing the appropriateness of access privileges, including the evaluation of privileges allowed within the application and database, and timely remove or adjust any inappropriate or unnecessary access detected to ensure that access privileges are compatible with employee job duties.

**Response:** The College will review and enhance its procedures to regularly review and update access to the College's computer system so that access and employee job duties stay congruent.

**Finding No. 3: Risk Assessment**

**Recommendation:** The College should develop a written, comprehensive IT risk assessment to provide a documented basis for managing IT-related risks.

**Response:** The College plans to have a written, comprehensive risk assessment program completed by June 30, 2012.

**Finding No. 4: Security Controls – User Authentication**

**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.

**Response:** The College will review and enhance its procedures regarding security controls related to user authentication.

Should you have any questions or concerns, please feel free to call me.

Sincerely,



Norman L. Stephens, Jr., Ed.D  
President

NS/ab

CC: David Blanton, Audit Supervisor

