REPORT NO. 2012-030
NOVEMBER 2011

TALLAHASSEE COMMUNITY 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
Eugene Lamb, Chair	Gadsden
Dr. J. Allison DeFoor, II, Vice Chair	Wakulla
Dr. Dana G. Callen	Leon
Bill J. Hebrock	Leon
Frank S. Messersmith	Wakulla
Dr. Kimberle Moon	Gadsden
Karen B. Moore	Leon

Dr. Barbara R. Sloan, President
to December 31, 2010 (1)

Dr. James T. Murdaugh, President
from November 15, 2010 (1)

Note: (1) Dr. Murdaugh was officially hired prior to the end of Dr. Sloan's term, and worked with Dr. Sloan during the transition period.

The audit team leader was Gregory A. Hunt, CPA, and the audit was supervised by Cheryl B. Pueschel, CPA. For the information technology portion of this audit, the audit team leader was Deidre Melton, CISA, and the supervisor was Heidi 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.

TALLAHASSEE COMMUNITY COLLEGE

SUMMARY

Our operational audit disclosed the following:

RECEIVABLES

Finding No. 1: The College needed to revise its procedures to provide for timely monitoring of recorded receivables.

EXPENSES AND DISBURSEMENTS

Finding No. 2: The College did not have written policies related to the use of electronic payments to vendors or for the use of electronic signatures, contrary to law.

INFORMATION TECHNOLOGY

Finding No. 3: The College did not always timely remove the access privileges of former employees.

Finding No. 4: The College did not retain some network access control records, contrary to the requirements of the State of Florida, *General Records Schedule*.

Finding No. 5: The College had not developed a written, comprehensive information technology (IT) risk assessment.

Finding No. 6: The College's security incident response procedures needed improvement with regard to the development of a trained security incident response team and the establishment of procedures for notifying parties affected by security incidents.

Finding No. 7: The College's security controls related to user authentication and data loss prevention needed improvement.

BACKGROUND

Tallahassee 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 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 campuses in Tallahassee, Florida. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Leon, Gadsden, and Wakulla Counties. The College reported enrollment of 11,975 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

Receivables

Finding No. 1: Accounts Receivable Collections

Effective internal controls over accounts receivables includes timely monitoring to ensure that amounts recorded as receivables are valid and recorded for the correct amount, and subsequent collections are properly recorded. We obtained the College's aged receivables report dated May 2, 2011, which included receivables from students, government agencies, and other entities totaling $2.5 million before any allowance for uncollectible accounts was applied.

Our review disclosed that improvements were needed in the College's procedures for monitoring and recording the collection of receivables from governmental and other entities. Our test included 50 of 480 account receivable transactions over a year past due, totaling $336,446. In addition, we requested documentation to support 281 account receivable transactions totaling $85,297, for amounts due from retiree's for health insurance coverage. Although requested, College personnel could not provide documentation to evidence that receivables recorded in the College's accounting records were valid amounts due to the College, were recorded for the correct amounts, or that the College had provided for timely follow-up on collections. Supporting documentation for the following transactions was not provided:

- For 48 receivable transactions totaling $276,718 that were over a year past due and recorded as due from the Florida Department of Health for reimbursements under various grants;
- An amount over two years past due from the Florida Department of Financial Services totaling $12,718, for training classes for another agency;
- An amount over a year past due from the Agency for Enterprise Information Technology totaling $47,010, for a training class; and
- Amounts due from 281 retirees for health insurance coverage transactions, totaling $85,297.

Subsequent to our inquiry, College personnel investigated these receivables and, as a result, $102,521 of the amount due from the Florida Department of Health, and $12,718 due from the Florida Department of Financial Services, has been collected. The receivable from the Agency for Enterprise Information Technology was removed by College personnel because they determined that the training class never occurred and the amount was not a valid receivable. The College determined that the amounts due from retirees for health insurance coverage were overstated by $81,484 due to errors in recording collections from retirees that should have been recorded as a reduction in the receivable balance. College personnel corrected the accounting records for these errors and indicated they will continue to review other receivables starting with the oldest receivables.

Timely monitoring of receivables reduces the risk of errors in the recording of amounts due to the College and enhances the College's ability to subsequently collect receivables.

Recommendation: The College should revise its procedures to provide for the timely monitoring of amounts due to the College.

Expenses and Disbursements

Finding No. 2: Electronic Payments

Section 1010.11, Florida Statutes, requires each college board of trustees to adopt written policies prescribing the accounting and control procedures upon 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. 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, approximately $8 million in electronic payments were made to various financial institutions and vendors for the purposes of transfers, investments, and payments of expenses during the 2010-11 fiscal year. The Board established policies that provide that the Board may authorize receipt or transfer of public funds to, from, or within its established bank accounts for the purpose of investments or direct deposit of funds provided that adequate internal control measures are established and maintained. However, the Board's policy does not address the transfer of public funds to other entities for the purpose of payment of College expenses. In addition, the Board's policies and procedures do not address the need for, or use of, electronic signatures when conducting electronic transactions between the College and other entities. While the College had established controls over electronic transactions, the lack of specific guidance in the Board of Trustee's policies increases the risk that electronic transactions will not be executed in accordance with Board directives and the provisions of Chapter 668, Florida Statutes.

Recommendation: The College should revise its policies to address the use of electronic payments as a means of payment for College expenses and the use of electronic signatures as discussed in Chapter 668, Florida Statutes.

Information Technology

Finding No. 3: Timely Removal of Access Privileges

Effective management of system access privileges includes the timely removal of employee information technology (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.

The College's procedures provide that when an employee terminates employment, the employee's department head or authorized representative submits a request to remove employee access privileges to the College's network, email, intranet, and the College's enterprise resource planning (ERP) application. The removal of access privileges to the College's network prevents former employees from being able to access the ERP application. The College established procedures that provide instructions for a programmer to remove ERP application access in addition to deleting network access. Our audit test of 91 employees who terminated employment from the College during the period July 1, 2010, through June 30, 2011, disclosed the following:

- ERP application access privileges for 10 former employees remained active from 158 to 413 days after termination of employment, contrary to the College's procedures. The College's ERP application software encompasses student, financial aid, finance, and human resource systems.

- Network access privileges for 3 former employees remained active from 77 to 385 days after termination of employment. The College's network allows access to certain critical application systems and confidential or sensitive information stored within documents of individual network users. Of the 3 former employees, 1 employee was among the 10 former employees described above whose ERP application access privileges had not been timely disabled or removed.

Although requested, the College was unable to determine whether the access privileges of the former employees had been used after the date of termination. Upon completion of access termination procedures, the College did not retain access control records of the employees. This matter is discussed further in Finding No. 4. When access privileges of former employees are not timely removed, there is an increased risk of unauthorized use, modification, or destruction of College data and IT resources by the former employees.

Recommendation: The College should ensure the timely removal of access privileges for former employees.

Finding No. 4: 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. Contrary to the *General Records Schedule* requirements, the College's procedures provided that an employee's network account was to be deleted from the system upon termination of employment. 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. 5: 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 considered external risks and identified security controls to mitigate these risks, it had not considered internal risks or developed a written, comprehensive IT risk assessment. 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 determining how IT-related risks, both external and internal, are managed.

Finding No. 6: 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 provisions for designated staff to be trained in incident response and notification to affected parties. Section 817.5681(1)(a), Florida Statutes, states that any person who conducts business in this State and maintains computerized data in a system that includes personal information shall provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement.

The College's security incident response plan did not include provisions for designated staff to be trained in incident response or procedures for the notification to affected parties required by Section 817.5681(1)(a), Florida Statutes. Should an event occur that involves the potential or actual compromise, loss, or destruction of College data or IT resources, the lack of a team trained in incident response and notification procedures could result in the College's failure to take appropriate and timely actions to prevent further loss or damage to the College's data and IT resources.

Recommendation: The College should revise its security incident response plan to require designated staff to be trained in security incident response and notification to affected parties of security incidents to provide reasonable assurance that the College will respond in a timely and appropriate manner to events, should they occur, that may jeopardize the confidentiality, integrity, or availability of data and IT resources.

Finding No. 7: 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 certain College security controls related to user authentication and data loss prevention 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 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

The College had taken corrective actions for findings included in our report No. 2010-027.

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 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. 2010-027. 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 database, operating system, network, and applications to determine the appropriateness based on the employees' job functions and responsibilities.
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.
Receivables.	Tested receivables to determine whether the receivables were properly authorized, documented, and within established limits. Determined adequacy of collection and write-off procedures.
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.
Student fee exemptions granted pursuant to Section 1009.25(3), Florida Statutes.	Tested students granted fee waivers and examined supporting documentation to determine whether College records for the fee waivers granted evidenced student eligibility and Board approval.
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.

EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Overtime payments.	Reviewed College policies, procedures, and supporting documentation evidencing the approval of and necessity for overtime payments.
Payroll and personnel.	Tested employees eligible for special termination benefits to determine that the liability and payment for these benefits were in accordance with Board of Trustee Rules and applicable Florida Statutes.
Procurement policies and procedures.	Tested purchases subject to competitive bids/proposals to determine compliance with bid requirements.
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.
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 a major construction project, tested payments and supporting documentation to determine compliance with College policies and procedures and provisions of law and rules. Also, for this construction management contract, 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 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

444 Appleyard Drive
Tallahassee Florida 32304-2895
850.201.6200 | *www.tcc.fl.edu*

November 17, 2011

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

Re: Operational Audit

Dear Mr. Martin:

In response to the preliminary and tentative audit findings related to your operational audit of Tallahassee Community College for the fiscal year ended June 30, 2011, we submit the following statements of explanation and correction.

Finding No. 1: Accounts Receivable Collections

Recommendation: The College should revise its procedures to provide for the timely monitoring of amounts due to the College.

Response: The College has revised its procedures to ensure continuous monitoring and timely collection of amounts due to the College. The Controller leads a monthly meeting with representatives from each office/department involved in creating invoices to ensure the timely receipt and follow-up on all outstanding invoices greater than 90 days. This procedure will continue to be ongoing to ensure timely monitoring and collection for outstanding receivables for the College.

Finding No. 2: Electronic Payments

Recommendation: The College should revise its policies to address the use of electronic payments as a means of payment for College expenses and the use of electronic signatures as discussed in Chapter 668, Florida Statutes.

Response: The College will revise policy 09-03 to address the use of electronic payments as a means of payment for College expenses and the use of electronic signatures as discussed in Chapter 668, Florida Statutes. During Spring 2012, the revised policy will be presented to the Board of Trustees for review and approval.

Finding No. 3: Timely Removal of Access Privileges

Recommendation: The College should ensure the timely removal of access privileges for former employees.

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

David W. Martin, CPA
Page Two

Response: The current process for removing network accounts has been revised. Once the employee is marked in the HR system as separating from the College, the network account is disabled. If the employee does not return within 12 months, the account will be deleted.

Finding No. 4: Access Control Records Retention

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

Response: The current process for removing network accounts has been revised. Once the employee is marked in the HR system as separating from the College, the network account is disabled. If the employee does not return within 12 months, the account will be deleted.

Finding No. 5: Risk Assessment

Recommendation: The College should develop a written, comprehensive IT risk assessment to provide a documented basis for determining how IT-related risks, both external and internal, are managed.

Response: By July 1, 2012, the College will develop a written, comprehensive IT risk assessment to provide a documented basis for determining how IT related risk, both external and internal, are managed.

Finding No. 6: Security Incident Response Plan

Recommendation: The College should revise its security incident response plan to require designated staff to be trained in security incident response and notification to affected parties of security incidents to provide reasonable assurance that the College will respond in a timely and appropriate manner to events, should they occur, that may jeopardize the confidentiality, integrity, or availability of data and IT resources.

Response: By April 1, 2012, the College will revise its security incident response plan to require designated staff to be trained in security incident responses and notifications to affected parties of security incidents.

Finding No. 7: Security Controls - User Authentication and Data Loss Prevention

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.

Response: As of October 27, 2011, the College has adopted a plan to improve security controls in relation to user authentication and data loss prevention.

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

David W. Martin, CPA
Page Three

We wish to express our appreciation to your staff for the professional and helpful manner in which they conducted the audit.

If I can be of further assistance, please do not hesitate to call me.

Sincerely,

Jim Murdaugh, Ph.D.
President