REPORT NO. 2012-032
NOVEMBER 2011

FLORIDA GATEWAY COLLEGE

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

BOARD OF TRUSTEES AND PRESIDENT

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

	County
Robert C. Brannan, III, Chair	Baker
Thomas M. Riherd, II, Vice Chair	Union
Donald R. Kennedy	Columbia
Kathryn L. McInnis	Dixie
Suzanne M. Norris	Columbia
Dr. Athena Randolph	Columbia
Julia Marcelle Richardson	Baker
Dr. James A. Surrency	Gilchrist
Harriet Wall to 9-14-10 (1)	Dixie

Dr. Charles W. Hall, President

Note: (1) Position remained vacant at June 30, 2011.

The audit team leader was Micah E. Rodgers, CPA, and the audit was supervised by Cathy L. Bandy, CPA. For the information technology portion of this audit, the audit team leader was Rebecca F. 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 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.

FLORIDA GATEWAY COLLEGE

SUMMARY

Our operational audit disclosed the following:

INFORMATION TECHNOLOGY

Finding No. 1: Some inappropriate or unnecessary access privileges existed within the College's information technology (IT) resources.

Finding No. 2: The College had not developed a written, comprehensive IT risk assessment.

Finding No. 3: The College did not have a written security incident response plan.

Finding No. 4: The College's IT security controls related to user authentication, account management, and data loss prevention needed improvement.

BACKGROUND

Florida Gateway 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 its main campus in Lake City, Florida, and a center in Baker County. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Baker, Columbia, Dixie, Gilchrist, and Union Counties. The College reported enrollment of 2,319 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

Information Technology

Finding No. 1: 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) application and the supporting operating system and database disclosed some accounts with access privileges that were in need of modification or removal to reduce the risk of unauthorized disclosure, modification, or destruction of College data and IT resources. Specifically:

- Seventeen application-delivered accounts had database administration privileges that were unnecessary or inappropriate. In addition, three database accounts used during a Fall 2009 conversion to a new financial application, though no longer necessary, were still active. In response to audit inquiry, College management removed the database administration privileges from the application-delivered accounts and deleted the database accounts used for conversion.
- Seven user accounts and five application-delivered accounts had update access privileges to critical transactions within the finance application module, including privileges for creating or modifying vendors, entering purchase orders and journal vouchers, processing invoices, and printing checks. This access was unnecessary or was contrary to an appropriate separation of duties. In response to audit inquiry, College management deleted a user account and removed the inappropriate access privileges from four of the remaining six user accounts. In addition, College management removed all application access privileges from the accounts.
- One application-delivered account utilized for the security administration of the application was shared by two employees, limiting the College's ability to assign responsibility for system actions taken using the account to a specific employee.
- One application-delivered class (grouping of access privileges) permitted users the unnecessary ability to set up electronic funds transfers. In response to audit inquiry, College management removed this ability from the class.
- Eleven user accounts and one application-delivered account had update access privileges to critical transactions within the HR module, including defining positions, inputting employees and rate of pay, modifying rate of pay, and entering time and pay adjustments. This access was inappropriate and was contrary to an appropriate separation of duties. In response to audit inquiry, College management removed the inappropriate access privileges from six of the user accounts and the application-delivered account.

Although the College performed a periodic review of employee access privileges, the College did not have written policies and procedures for reviewing access privileges. The existence of the incompatible or unnecessary access privileges described above indicated a need for enhanced procedures for 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 establish written policies and procedures for reviewing the appropriateness of access privileges, including privileges within the application and database, and timely remove or adjust any inappropriate or unnecessary access detected.

Finding No. 2: 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, it had not developed a written, comprehensive IT risk assessment. According to College personnel, the Florida College System (comprised of 28 Florida Colleges, including Florida Gateway College) 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, that the most significant risks have been addressed, and that 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 are to be managed.

Finding No. 3: Security Incident Response Plan

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

The College did not have a written security incident response plan. As noted above, the College has 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 create, execute, and maintain security incident response procedures. Should an event occur that involves the potential or actual compromise, loss, or destruction of College data or IT resources, the lack of a written security incident response plan could result in the College's failure to take appropriate and timely action to prevent further loss or damage to the College's data and IT resources.

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

Finding No. 4: Security Controls – User Authentication, Account Management, 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, account management, 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, account management, 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, account management, 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 action for the finding included in our report No. 2010-019.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this operational audit from March 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. 2010-019. 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.	Determined whether a written security incident response plan had been developed.
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.
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.
Purchasing card transactions.	Tested transactions to determine whether the 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.
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.
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.
Construction administration.	For a selected major construction project, tested payments and supporting documentation to determine compliance with College policies and procedures and provisions of laws and rules.
Overtime payments.	Reviewed College policies, procedures, and supporting documentation evidencing the approval of and necessity for overtime payments.

EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
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.
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.
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.
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.

EXHIBIT B
MANAGEMENT'S RESPONSE

FLORIDA GATEWAY COLLEGE

November 21, 2011

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

Dear Mr. Martin:

In response to the preliminary and tentative audit findings and recommendations from your audit of the District Board of Trustees of Florida Gateway College for the Fiscal Year Ended June 30, 2011, we submit the following comment's including corrective action taken or to be taken.

Finding No. 1: Some inappropriate or unnecessary access privileges existed within the College's information technology (IT) resources.

Recommendation: The College should establish written policies and procedures for reviewing the appropriateness of access privileges, including privileges within the application and database, and timely remove or adjust any inappropriate or unnecessary access detected.

Response: The College has contracted with a third party consulting group to review job responsibilities in correlation to access privileges and make adjustments as necessary. Upon completion of task, the College will develop policies and procedures for continued maintenance of these privileges.

Finding No. 2: The College had not developed a written, comprehensive IT risk assessment.

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

Response: The Florida College System CIO's in conjunction with IBM have developed an FCS IT Security Strategic Direction Plan that outlines defining and implementing a Security Risk Management program. The College will use this document to guide the implementation of said plan.

149 S.E. College Place
Lake City, FL 32025-2007
(386) 752-1822
www.fgc.edu

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Mr. David W. Martin, CPA
Page 2
November 21, 2011

Finding No. 3: The College did not have a written security incident response plan.

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

Response: The College will use the FCS IT Security Strategic Direction Plan to guide the implementation of a Security Incident Response plan.

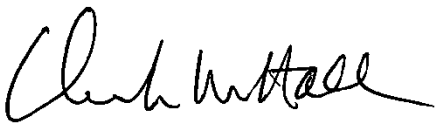
Finding No. 4: The College's security controls related to user authentication, account management and data loss prevention needed improvement.

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

Response: The College fully supports appropriate security controls to protect the confidentiality, integrity and availability of data and IT resources. The College will review the recommendations for improving security controls and make changes as appropriate.

If you have any questions, please contact Marilyn Hamm at 386-754-4364 or Mike Davis at 386-754-4242

Sincerely,



Dr. Charles Hall, Ed.D
President

:bc