FEBRUARY 2002 REPORT NO. 02-138

AUDITOR GENERAL

WILLIAM O. MONROE, CPA

FLORIDA COMMUNITY COLLEGE AT JACKSONVILLE
ORION SYSTEM

INFORMATION TECHNOLOGY AUDIT
For the Period April 30, 2001, Through August 13, 2001
And Selected College Actions Taken Through November 19, 2001

SUMMARY

Our audit focused on management controls and selected information technology functions applicable to the Orion System at the Florida Community College at Jacksonville (the College) during the period April 30, 2001, through August 13, 2001.

The Orion System is the College's enterprise software system providing college-wide administrative and instructional support.

Deficiencies were noted in the College's access, application, and general management controls related to the Orion System. Specifically, these matters included:

- ***Lack of policies and procedures defining operations, roles, and responsibilities of Information Systems Support;***
- ***Inadequate safeguards imposed for the Data and Network Operations Center and inadequate network back-up procedures;***
- ***Inadequate preparation for prolonged service interruption through a written comprehensive Disaster Recovery Plan;***
- ***Functional and reporting deficiencies in the Orion System's fundamental financial processing resulting in increased manual procedures and duplicative effort for reconciliation;***
- ***Inadequate time for the College's batch job processing needs; and***
- ***Deficiencies in the College's information security controls applicable to the Orion System.***

Background:

With more than 55,000 students enrolled, Florida Community College is the second largest community college in the State. The College is a member of the Florida Community College Software Consortium, a group of seven Florida community colleges organized to produce a software package to process, track, and report the colleges' administrative and instructional transactions. The six other Consortium members include: Miami-Dade, Broward, Palm Beach, Indian River, Okaloosa-Walton, and Tallahassee community colleges. In 1995, the Consortium received State funding through additional budget appropriations to each member college to begin development of the Enterprise Resource Planning software, Integrow. A suite of application components developed in Natural and Construct programming languages, Integrow includes the Student Information system; Financial Information system, comprised of general ledger, credit and collections, purchasing and receiving, accounts payable, and budget modules; Personnel and Payroll system; Facilities system; and Security system. As implemented and operated at the College, the Integrow package is called the Orion System.

The College began implementation of the Facilities system on January 1998 followed by the Financial Information system and Personnel and Payroll system in June 1998. The Student Information system was operational in May 1999. The College successfully completed a cycle of all processes within the new system, including the Financial Aid component, by March 2001.

The College utilizes a separate financial aid package, Financier, developed by WolffPack to maintain and track the progress of financial aid applications and awards to students. The Consortium supports Financier's integration with Integrow for those members using Financier.

The Orion System operates on a mainframe platform. Faculty and student access to the Orion System via the Internet is permitted through the Academic Resource Technology and Education Management Information System (Artemis) web-based portal. The Orion System serves as the transaction and data engine for Artemis running on a server-based platform. Through Artemis, students can conduct necessary business such as registration, payment remission, and demographic information changes with the College using simple browser technology. Faculty may view course catalogs, class schedules, personal schedules, and class rolls and provide links to server-based syllabi.

The College is a charter member of the Service-members Opportunity Colleges, a national consortium of 400 colleges. Accordingly, the College maintains a contract with the Navy to provide academic advising and curriculum services to students deployed world-wide under the Navy College Partners Program**.**

The Information Technology (IT) Department operates under a department-defined mission to create a powerful and highly reliable technological environment with an expanded support role to include the enablement of the instructional and learning-centered processes of the College. The IT Department is divided into three main areas: Educational Technology, E-Systems Technology, and Management Information Systems and Decision Support (Information Systems Support). Functions served by Information Systems Support include application and systems programming, operations and production control, and database administration. Educational Technology, separated into Academic Systems and Advanced Technology, is largely responsible for the configuration and support of the College's network infrastructure and systems. In May 2001, the College hired a Data Security Specialist whose initial duties included documenting security procedures and network account management. E-Systems Technology designs and maintains the College's Web presence and Internet-based applications.

At the time of our initial fieldwork, the Enterprise Systems Group within Information System Support made changes to the standard application baseline resulting from user requests. Subsequently, the College's Vice President of Technology and Chief Information Officer (CIO) indicated that, as of November 19, 2001, the College no longer performs system development or enhancement activities for the Orion System except as part of the Consortium project team working within the Consortium's procedures. The programming staff within the Enterprise Systems Group may create a fix or patch while the Consortium is developing a baseline change. They may also code reports for College staff. Our audit scope did not include an evaluation of Consortium methodology, policies, or procedures regarding system development and modification activities.

A port, often derived from requests submitted by Consortium member users, is a change made by the Consortium to the baseline application. The Consortium's Executive Committee enacted a policy whereby each participating college must have the most current version of development tools supporting the Integrow software, according to Consortium specifications, in order to accept new ports. If the colleges do not maintain the applicable versions, they will not receive the ports.

Key users within Admissions, Records and Registration, Budget and Payroll, Controller, Human Resources, and Financial Aid offices have been designated the functional owners of the respective Orion System components. Further, selected key users serve as Security Administrators for the Financial, Student, Personnel and Payroll, Facilities, and Financial Aid component modules approving and establishing user access.

Finding No. 1:

IT management had not formulated policies and procedures defining operations, roles, and responsibilities of Information Systems Support.

As with other essential business functions of an entity, the IT organization should be guided by policies and procedures describing the scope of its function, activities, and interrelationships with other departments. Policies and procedures establish the organization's direction and provide benchmarks against which compliance can be measured and contribute to an effective control environment.

There were no formal policies and procedures written to define management's expectations for applicable system maintenance, operations and production control, system back-up and recovery, data center access control, system logging and review, and following up on exceptions and problems activities. The absence of defined policies and procedures reduces management's assurance that controls and measures necessary for the consistent and continued achievement of intended goals and initiatives will be performed.

Recommendation:

The College should formally define, document, and distribute policies and procedures necessary to achieve management's objectives with regard to assigned Information Systems Support functions.

Finding No. 2:

The College did not have in place adequate environmental and physical safeguards for the Data and Network Operations Center nor adequate network back-up procedures.

IT management should ensure that sufficient specialized equipment and monitoring device measures are installed and maintained for protection against environmental factors. Further, sensitive areas should be identified and authorization procedures controlled and monitored to ensure secured access. Back-up procedures for IT-related media should include secured off-site storage of data files, software, and related documentation.

Deficiencies were noted in environmental controls for the mainframe, network, and uninterruptible power supply (UPS) rooms and physical security controls as follows:

- The Data and Network Operations Center maintained two air conditioning and humidity controllers to regulate the air in both the network and the mainframe rooms. However, neither machine contained a monitoring device to notify personnel of a problem.
- Smoke detection equipment was not present within the Data and Network Operations Center.
- Neither the network room nor the mainframe rooms had water detection devices underneath the raised floors.
- Sprinkler systems had been installed in the ceilings above the network, mainframe, and UPS equipment. However, the College had not formalized response procedures or guaranteed vendor provided assistance in the event of sustained water damage to the equipment.
- The College had not, in all instances, appropriately restricted physical access to the mainframe and network equipment. Access to the mainframe and network room was based on an assigned security status level. Assigned status level determined whether the card key permitted access to the mainframe room, network room, or both. However, management had not defined, by position, assignment of the respective security levels. Our audit disclosed that one Lead Courseware Support Analyst, and two Database Administrators unnecessarily had access to the mainframe room. Additionally, the Lead Courseware Support Analyst and Systems Programmers were unnecessarily permitted access to the network room based on the type of equipment contained therein.

Additionally, while full network back-ups were scheduled throughout the week for each critical server, these back-ups were not stored at the off-site vault along with the enterprise data back-ups.

Subsequent to our field work, the College indicated that sensors and monitors had been added for smoke and water detection with automatic notification to system administrators via pager. Additionally, College management indicated the removal of access to the mainframe or network rooms for the aforementioned personnel. Further, the College initiated plans to reschedule the full network back-ups in order to be taken off-site as well.

Without sound physical access controls and environmental hazard safeguards, data center resources, equipment, and data may not be sufficiently protected from compromise, failure, or service disruption. Further, not securing all critical back-ups off-site exposes risk to the College's continued operations through timely managed information systems data and resources availability.

Recommendation:

The College should implement and maintain environmental controls as noted above to ensure the safety of data center resources from environmental hazards. Additionally, the College should continue plans to ensure off-site storage of network back-ups. Further, the College

should enact policy whereby access to data center equipment is authorized with regard to specific job duties.

Finding No. 3:

The College had not adequately prepared for prolonged service interruption through a written comprehensive Disaster Recovery Plan.

A quality contingency plan should document an organization's detailed recovery procedures sufficient to quickly and smoothly restore processing capabilities in the event the computer or communications facility becomes inoperable or inaccessible.

The College drafted a proposed disaster recovery plan primarily addressing payroll processing procedures. The plan also cited enterprise system back-up procedures and reflected a signed agreement with Tallahassee Community College as an alternate processing site. However, the draft plan did not include provisions for the finance, financial aid, student, or personnel processing components of the enterprise system and therefore, restoration of its critical business purpose. Additionally, the proposed draft did not include provisions for network server and data recovery or replacement and overall network restoration. As the plan remained in draft, testing procedures had not been conducted.

Without a Disaster Recovery Plan detailing provisions and necessary steps to continue all critical operations during a prolonged disruption, the College's risk is increased of untimely recovery of service delivery and sustained losses.

Recommendation:

The College should expand its disaster planning efforts to address recovery procedures for all enterprise system components critical to timely restoring the College's operations. The plan should be periodically reviewed, updated, and tested to reflect current business practices, operations, equipment, and personnel, and to ensure adequacy of recovery procedures.

Finding No. 4:

Functional and reporting deficiencies in the Orion System's fundamental financial processing resulted in increased manual procedures and duplicative effort for reconciliation.

Data integrity is of greater concern in an integrated system due to the broader potential impact of erroneous data on the organization. Risks associated with financial reporting include subsidiary ledgers that are not in balance with the general ledger and transactions not posted at all or not posted to proper accounts. Key control features of financial reporting include providing control totals and record counts for transactions processed, validating that transactions are in balance, and generating interface control reports for reconciliation of ledger feeds. Key control features for subsidiary components include producing reports and information for balancing subsidiary detail and general ledger control accounts, and detailing the general ledger interface and the subsidiary balance changes.

Our audit noted the following deficiencies:

- As the College detected instances where the Orion System did not post an entry or double posted an entry during nightly batch processing, the Accounts Payable Manager performed a daily manual reconciliation of the accounts payable subsidiary records with the general ledger records. Often, errors resulted from invoice or credit memo cancellations. Consortium staff believed the cause to be the ordering of program statements, within the invoicing module, used to ensure edits and updates of different files were performed. The Consortium indicated that the problem has been addressed in a subsequent port.

- Daily, the Accounts Receivable Accountant created a spreadsheet of beginning balances from the credit and collections and general ledger modules and reconciled the differences between them for each account. Differences were noted in various retiree insurance premium account balances resulting from the Orion software implementation process. Additionally, differences between general ledger and credit and collections modules occurred in the Accounts Receivable – Tuition account. The account balance differences were caused by cashiering sessions that had not been closed prior to nightly batch processing. Open sessions could involve cashier workstations, registration terminals, and web and touchtone registration sessions. The system could not post amounts to the general ledger until cashiering sessions were closed.

- A financial aid run, posting disbursements from the financial aid module to the credit and collections module, was accompanied by a report listing disbursements not carried over to credit and collections. The report, first used by the College in 2001, was cumulative since the implementation of Financier in 1999 and, as of June 19, 2001, contained 117 exceptions. The report did not provide a total amount of rejected disbursements. Subsequent to our fieldwork, the College indicated that the causes of all but one of the exceptions had been determined and correcting entries, where required, had been made.

Discrepancies between system components resulting from processing or posting errors creates the need for extended time and effort of personnel resources to trace transaction errors and determine necessary correction procedures. Consequently, the College risks inaccurate and untimely financial or management reporting.

Recommendation:

The College should request that the Consortium provide corrections to system processing, as appropriate, and develop enhanced reporting tools, including the use of control totals between modules, to alleviate manual reconciliation procedures redundant to system intended processing.

Finding No. 5:

The College experienced contention between on-line and batch processing service provision.

The level and quality of service provided by a data center is based largely on user perceptions of the availability of the application and the timely receipt of scheduled reports.

Workload demand must be balanced to ensure that adequate capacity is available and that best and optimal use is made of resources to meet required performance needs.

Generally, the Orion System is brought down nightly beginning at 10:00 p.m. for batch processing. During this time, the Orion System resources are closed to Artemis and the touchtone registration system as well. The IT Department has made a commitment to the College to have Orion on-line no later than 7:00 a.m.

Although staff reliant on nightly processing tried to organize the schedule to make the best use of the time available, needed jobs were sometimes postponed in an effort not to overrun the nightly batch window. Additionally, completion of jobs already in progress caused delay in bringing the system on-line by the 7:00 a.m. deadline. IT management indicated that causes of the inability to complete nightly processing within the allotted window included management's desire, pursuant to its Navy contract, to keep online systems up for student registration and payment access via Artemis; the limited number of checkpoints designed into the system allowing for quicker error recovery by allowing a restart at the last checkpoint rather than the beginning of the job; and the large volume of jobs to be run at certain times of the year. Month-end processing usually lasted until after 7:00 am. Additionally, from approximately one week before the start of each term until approximately two weeks after the start of the term, the online system was late coming up in the morning two or three times a week. IT management stated that it intends to explore the possibility of performing some daytime batch processing as a solution.

Compressing the nightly batch processing window in an effort to increase system availability for student services may impair the College's administrative functions. As users are prohibited entry into Orion during batch processing, they may not achieve their normal work product when conditions arise which prevent the system from returning to on-line status at the appropriate time. If inadequate time is provided in which to run the batch processes, jobs necessary to the continued operations of the College may not be performed.

Recommendation:

College management representing both the user community and IT should work toward defining a service level agreement for system processing and availability that will allow the College to honor its commitment to student users as well as achieve its business and operations objectives. The College should also continue to explore available options for maximizing processing efficiency.

Finding No. 6:

Deficiencies were noted in the College's information security controls applicable to the Orion System.

Effective security relies on a security structure that includes operational policies, organization and resources, user awareness, and security administration procedures. Specific procedures should be developed for each of the major functions of security administration including designing the security hierarchy; granting and revoking system access; granting and revoking data and resource access; and reporting and monitoring activity. Employees should receive and acknowledge documentation describing security policies, procedures, individual responsibilities, and the consequences of security violations.

IT and user management had not developed policies and procedures formally defining roles and responsibilities to maintain consistent user account management, security administration, access distribution, and system security standards. In addition, the College's information security practices were deficient in the following areas:

- Certain important security features had not been utilized. Specific details of these security deficiencies are not disclosed in this report to avoid any possibility of compromising College information. However, appropriate College personnel have been notified of these deficiencies.
- The College had not implemented a formal security awareness program for its staff nor required users to acknowledge in writing that they have been presented with, understood, and agree to comply with security policies. The College published computing policies covering software piracy, facilities policies, and user agreements for students, employees, and all other users of College computing facilities in its College Catalog. According to the College's Vice-President of Technology and CIO, the College assumed anyone using computing facilities, accepting employment, or registering as a student agreed with policy terms.
- Procedures for creating, managing, and deleting user accounts were not consistently applied. Generally, requests for user account creation and notification of terminations should be submitted through the Learner Support Center (Help Desk). However, the procedure was sometimes bypassed with requests or notifications sent to Courseware Support under Educational Technology within IT. User account requests addressed through Courseware Support were not required to be formally documented. Notice of employee separation from employment was reported to Courseware Support directly or not reported to either the Help Desk or Courseware Support. Additionally, there was no monitoring procedure to ensure that the separated employee's access had been revoked. User accounts were not always disabled or deleted, but rather reused as the user's account could be tied to course material access or the execution of system processing jobs. We noted during our audit an instance of a programmer's use of a former employee's user account having assigned access authority greater than that needed by the programmer. The programmer had been assigned his own user account as well.
- Contrary to stated College practice, alias access authority extended beyond a period of one year. Within the Orion System, budget managers designated an alias(es) to approve documents during their absence. Within the Orion System, a user already having security access to the approval system within the Financial Information system, could be delegated the same access authority as the budget manager for a defined start and end date. While there were no formal policies and procedures addressing the delegation and duration of alias access authority, the Assistant Controller stated that the established period for an alias should be confined to a fiscal year. Our review of selected alias access privileges noted instances where alias access authority had been defined for periods ranging from 13 months to 220 years.
- Our review of the Security Matrix Report displaying the College's users and the Orion System components defined to their profiles disclosed excessive distribution of access to the Security system. Modules within Security could not be assigned to a user without the system defined to the user profile. Although a created link between the user and the modules was necessary within Security, the College stated that a user with access to one module and also access to Security, generally had the ability to grant access to all systems within Orion.
- Due to the design of Orion's Security system, designated Security Administrators and back-up administrators for each Orion System application component had access to and could assign access to all Orion System components. Therefore, each Security Administrator and back-up administrator could function as a security super user. The practice of allowing multiple individuals the security super user capability may lessen the

College's assurance that system access will be granted as appropriately authorized.

- The Security Matrix Report did not detail user access by system, module, and functions within each module. Consequently, periodic detailed security reviews were not conducted by the College for the purpose of ascertaining continued appropriateness of user access rights and privileges.
- Several Payroll employees had assigned access authority within personnel modules within the Personnel and Payroll system. Modification or update to these modules could be performed in the course of daily responsibilities or could be necessary to continue payroll processing. Inadequate segregation of personnel and payroll functions through system access controls increases the risk for data compromise without timely detection.
- The College had not determined who should be authorized to override specific holds on student registration. Currently, Registrar's office, campus enrollment services, and counseling personnel; instructors; deans; and departmental secretaries throughout the College may have override capability. The College's Administrative Procedure Number 10-0802 provided that registration restrictions would be cleared by "authorized personnel". In September 2000, a hold override committee was formed. This committee, composed of college-wide representation, was charged to provide registration override capability to college staff within the scope of their job responsibility. Following the committee's decisions as to whom override authorization would be granted, Orion system security would be changed to restrict override to those persons identified by the committee. However, the committee did not plan to meet until February 2002. Without identification of appropriate parties and proper authorization for use of student hold overrides, the College may not be assured that policy introduced to control student registration in accordance with legal or regulatory requirements will not be circumvented.

Absent formal security administration procedures, the risk exists that the confidentiality, availability, and integrity of College data and information technology resources could be compromised and not be timely detected. Deficiency with regard to periodic user review increases the risk that access granted inadvertently or privileges that are no longer relevant may not be recognized and timely corrected. Further, a lack of acknowledgement and accountability by all users responsible for data may expose the College to the risk of information breach without consequence to the violating party.

Recommendation:

The College should implement stronger security features in the areas noted above. Specifically, the College should designate, approve, and implement formal procedures and standard system controls to be used by authorized personnel assigned security administration tasks. The College should also establish one security super user and back-up with the ability to grant access to all systems based on authorization of the systems' functional owners. Additionally, users should be informed of their responsibility in maintaining the confidentiality, integrity, and availability of the data entrusted to them. Further, careful monitoring of personnel and payroll functions should be required to ensure appropriate segregation of duties.

Other Matters:

The United States Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, which addresses electronic data interchange, privacy, and information security standards for personal health information. HIPAA also provides for civil and criminal penalties for noncompliance. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards and privacy with security regulations expected to be published in 2002. The College, in offering employees health insurance through a provider and as a participant in health career programs, recognizes the applicability of HIPAA. The College has not defined a formal plan in response to pending HIPAA regulations. Although the College indicated that it does not transmit any data concerning the health status of employees, their dependents, or students, the privacy and security rules under HIPAA may significantly influence procedures with regard to the handling of health records. Accordingly, advance planning to evaluate the impact of the HIPAA requirements on the College will serve to reduce the difficulties in making the necessary transition to comply with these requirements.

Scope, Objectives, and Methodology:

The scope of this audit focused on evaluating selected information technology functions applicable to the Orion System during the period April 30, 2001, through August 13, 2001. Our objectives were to determine the effectiveness of selected general and application controls relating to the Orion System.

To meet our audit objectives, we reviewed applicable Florida Statutes, administrative rules, and auditing literature; interviewed appropriate College personnel; obtained an understanding of management controls relating to selected information systems functions; observed controls processes and procedures; and, performed various other audit procedures to test selected controls related to the Orion System.

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 audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

College Response:

In a response letter dated January 30, 2002, the President of the College generally concurred with our audit findings and recommendations. The College's response can be viewed in its entirety on the Auditor General Web Site.

We conducted our audit in accordance with applicable standards contained in Government Auditing Standards ***issued by the Comptroller General of the United States. This audit was conducted by Heidi G. Burns, CPA*, CISA, and supervised by Nancy M. Reeder, CPA*, CISA. Please contact Jon Ingram, CPA*, CISA, Audit Manager, with any questions regarding this report. He may be reached via e-mail at joningram@aud.state.fl.us or by telephone at*** *(850) 488-0840.*

This report and other Auditor General reports can be obtained on our Web site **(www.state.fl.us/audgen)**; *by telephone at* ***(850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).***

**Regulated by State of Florida*

FLORIDA
COMMUNITY
COLLEGE
AT JACKSONVILLE

Dr. Steven R. Wallace
College President

January 30, 2002

William O. Monroe, CPA
Auditor General, State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe:

The purpose of this letter is to acknowledge and respond to the findings of the audit of Florida Community College at Jacksonville's ORION System for the period April 30, 2001 through November 19, 2001 conducted by your office.

College Response to Finding 1:
Although not in policy/procedure form, the roles and responsibilities of all I.T. staff and functional areas are clearly communicated in the I.T. business plan, which resides on the web. Expectations and benchmarks are expressed and measured in the form of project plans that cover all I.T. tasks. Additionally, constant monitoring of help desk ticket close rates is included in evaluation of performance for each area. The collegewide initiatives-based planning model serves as the basis for alignment between I.T. and the greater college. Each initiative includes specific deliverables, assigned responsibility, and regular status report. The I.T. management team will begin development of these items in procedure form.

College Response to Finding 2:
The College implemented environmental controls consistent with those recommended in November 2001.

College Response to Finding 3:
Based on risk assessment and cost-benefit analysis, it was determined that payroll was the most time-critical system at the College and most directly affected college operations. Therefore, payroll was the first system for which immediate operation recovery was planned. Work has been in progress for nearly two years to develop and implement a dependable and cost-effective solution for disaster recovery for all systems. This is a complex and expensive issue due to the size of the databases, integrated nature of the systems, and unique environment at FCCJ. I.T. staff has issued a RFP for security (and disaster recovery) and plans to recommend a plan for funding during the FY 02-03 budget development cycle (Spring 2002).

College Response to Finding 4:
The College requested that the Consortium provide corrections to system processing as appropriate. The Consortium is in the process of developing those corrections.

College Response to Finding 5:
The service level has been determined and published. The College is awaiting FCCSC modifications, which will enable simultaneous batch and on-line processing in ORION necessary to meeting the stated service levels. Service levels will be developed into a procedure form.

College Response to Finding 6:
I.T. staff has issued an RFP for a security management solutions provider for assistance in this area. Lack of staff and funding has been the primary impediment for college-specific security. Changes to ORION's security are in development at the FCCSC.
A new account creation and management system for all FCCJ systems has been in development for the past year and should be complete by fall term 2002.

We at Florida Community College appreciate the thoroughness and professionalism with which this audit was conducted and will make productive use of the findings.

Best regards,

Steven Wallace

Dr. Steven R. Wallace
College President

C: Mr. Steve Bowers
Dr. Rob Rennie