FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of the PantherCARD Financial, Operational, and Information Systems Controls

Report No. 11/12-02

August 8, 2011

FIU | FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: August 8, 2011

To: Kenneth A. Jessell, Chief Financial Officer & Senior Vice President
Liane Martinez, Associate VP Strategic Development/Financial Planning

From: Allen Vann, Audit Director

Subject: **Audit of the PantherCARD Financial, Operational, and Information Systems Controls, Report No. 11/12-02**

We have completed an audit of the PantherCARD Financial, Operational, and Information Systems (IS) Controls. The PantherCARD is a computerized identification card system that uses photo imaging technology and an encoded magnetic strip that allows cardholders to open a debit account, for use at various on campus vendors to purchase food, books, and other goods and services. The card is also used for access into buildings and admittance to FIU football games. During our audit period, there were over 184,000 accounts worth almost $2.3 million and transaction flows of $4.5 million in deposits, net of refunds, and $4.2 million in outflows to vendors. On April 15, 2011, the University announced the FIU One Card program, replacing the PantherCARD and offering a variety of additional financial benefits to students, faculty and staff. The One Card will continue to offer an FIU debit account for internal campus usage, as well as the option to link the card to a Wells Fargo checking account.

Overall, our review over the F*inancial Controls* over PantherCARDs disclosed some areas of concern, including the accounting for transactions, procedures allowing for the immediate availability of funds to cardholders without first securing the funds, procedures for dormant accounts, and excessive access to sensitive student banking data. Additionally, our audit identified some areas in need of improvement, particularly in the manner vendor payments are processed; the process by which copy cards are issued and used; the cardholder refund process; how cardholder deposits are accepted, processed and deposited; and the terms and conditions in contractual agreements with vendors regarding PantherCARD processing.

Operational Controls reviewed card stock physical security and inventory, card lifecycle, from creation to deactivation, and the cards use for building access. With the exception of card lifecycle processes which were found to be satisfactory, the operational controls over PantherCARDs identified areas in need of improvement, particularly in the use of temporary PantherCARDs; the need for electronic backup of inventory logs; and the accessibility to the Inventory Log File.

As for *Information System Controls*, we determined that the PantherCARD Office needed to develop and formally document access controls and procedures for CS Gold. It is not evident that user accounts were being properly managed. Temporary, terminated employees, and emergency accounts need better management. We found that unnecessary application privileges were granted to individual and vendor accounts which resulted in providing greater privileges than needed for the individuals to perform their related job functions. A single user with excess application privileges could circumvent existing controls and perform a malevolent act. There were also deficiencies in workstation security that could potentially allow the installation of malicious software thereby increasing the risk of data loss or network disruption. Finally, a Business Continuity Plan would protect the integrity of PantherCARD data and minimize the financial impact resulting from unexpected events.

The audit resulted in 49 recommendations, which management agreed to implement.

We wish to express our appreciation for the cooperation and courtesies extended to us by the PantherCARD Office, Controller's Office, the Office of Business Services, and all those dealt with while conducting the audit.

C: Sukrit Agrawal, Chair, Board of Trustees & Finance and Audit Committee Members
Richard Brilliant, Treasurer and Chair, FIU Foundation Finance & Audit Committee
Mark B. Rosenberg, University President
Jeffrey Krablin, Assistant Vice President, Business Services

TABLE OF CONTENTS

BACKGROUND

The FIU PantherCARD is a computerized identification card system which uses photo imaging technology and an encoded magnetic strip. The card was introduced to students in 1993 and to faculty/staff in 1994. The system allows cardholders to open a debit account, which they can then deposit monies into for use at various University vendors to purchase food, books, and other goods and services on campus. The card is now also used for access into buildings, admittance to FIU football games, and other services. Currently, there are approximately 17 plans which cardholders can participate in. The PantherCARD Office administers the system which these programs run on, known as CS Gold.

The PantherCARD Office, which was part of the University's Graham Center during the audit period, was transferred to the Business Services Office at the end of February 2011. Transactions are recorded in the University's Auxiliary Trust Fund. As of December 31, 2010, there were over 184,000 accounts consisting of almost $2,250,000 in balances. Included in these balances were approximately 117,000 accounts for Business Services copy cards, totaling $134,300. Copy cards can be purchased at various locations and while primarily intended for photocopying, may be used throughout University for other goods and services. These copy cards are initially purchased by Business Services but funds are administered by the PantherCARD Office.

On April 15, 2011, the University announced the FIU One Card program, which would replace the PantherCARD and offer a variety of benefits to students, faculty and staff. The One Card will continue to offer an FIU debit account for internal campus usage, as well as the option to link the card to a Wells Fargo checking account. Wells Fargo opened a full-service branch at the University this summer to serve the students, faculty and staff. The new One Card will have the ability to be used as a debit card at all retail locations that accept pin-based transactions on and off campus.

The PantherCARD Office remained in the Graham Center with all operations remaining unchanged through July 15, 2011. On July 18, 2011 the FIU One Card relocated adjacent to the new Wells Fargo branch and began issuing the new FIU One Card to all incoming freshman and transfer students. A re-carding effort will take place during fall semester 2011 for all faculty, staff, and continuing students to replace their current card with the new FIU One Card.

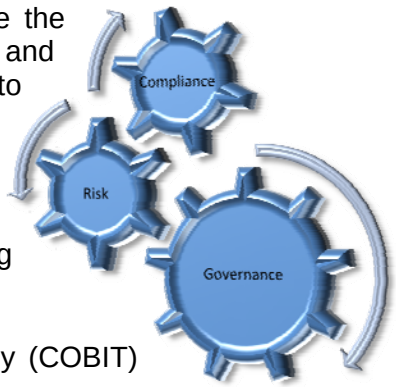
OBJECTIVES, SCOPE, AND METHODOLOGIES

The objectives of our audit of the PantherCARD Financial, Operational, and Information Systems (IS) Controls are to determine: (1) whether established internal controls over card distribution and financial transactions are adequate and effective and operated in accordance with established University policies and procedures, applicable laws, rules and regulations; (2) whether sufficient IS controls are in place over processing, storing, safeguarding and/or transmittal of data contained in the PantherCARD system; and (3) the security related risks associated with PantherCARD Access Privileges.

Our audit included the PantherCARD transactions handled by the PantherCARD Office for the period from January 1, 2010 through December 31, 2010 and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*, and included tests of the accounting records and such other auditing procedures as we considered necessary under the circumstances. Audit fieldwork was conducted from January 2011 to May 2011.

During the audit, we reviewed University policies and procedures, and applicable Florida Statutes, observed current practices and processing techniques, interviewed responsible personnel, confirmed student withdrawal transactions, and tested the selected transactions. Sample sizes and transactions selected for testing were determined on a judgmental basis. PantherCARD processed $4.5 million in deposits, net of refunds, and paid out $4.2 million to vendors during the scope period.

We identified and tested key internal control objectives[1] to determine the effectiveness of existing controls. We also reviewed past internal and external audits, which included prior Recommendations: related to PantherCARD Financial and Information Systems Controls to determine whether management had effectively addressed prior audit concerns.



To achieve our IS audit objectives, we applied the following Methodologies and Guidelines:

- The Control Objectives for Information and related Technology (COBIT) 4.1 Framework).
- The National Institute of Standards and Technology Special Publication (NIST) 800-53A Revision 1 Guidelines.
- Payment Card Industry Data Security Standard (PCI-DSS) Version 2.0.

[1] Discrete control procedures or controls are defined by the SEC as: "...a specific set of policies, procedures, and activities designed to meet an objective. A control may exist within a designated function or activity in a process. A control's impact...may be entity-wide or specific to an account balance, class of transactions, or application. Controls have unique characteristics – for example, they can be: automated or manual; reconciliations; segregation of duties; review and approval authorizations; safeguarding and accountability of assets; preventing or detecting error or fraud. Controls within a process may consist of financial reporting controls and operational controls (that is, those designed to achieve operational objectives)."

FINDINGS AND RECOMMENDATIONS

Our report on the management of the PantherCARD program is divided into three distinct sections: Financial Controls, Operational Controls, and Information System Controls. Details follow.

Financial Controls

Overall, our review over the financial controls over PantherCARDs disclosed some areas of concern, including the accounting for transactions, procedures allowing for the immediate availability of funds to cardholders without first securing the funds, procedures for dormant accounts, and excessive access to sensitive student banking data.

Additionally, our audit identified some areas in need of improvement, particularly in the manner vendor payments are processed; the process by which copy cards are issued and used; the cardholder refund process; how cardholder deposits are accepted, processed and deposited; and the terms and conditions in contractual agreements with vendors regarding PantherCARD processing.

Our overall evaluation of internal controls for PantherCARD Financial Controls is summarized in the table below.

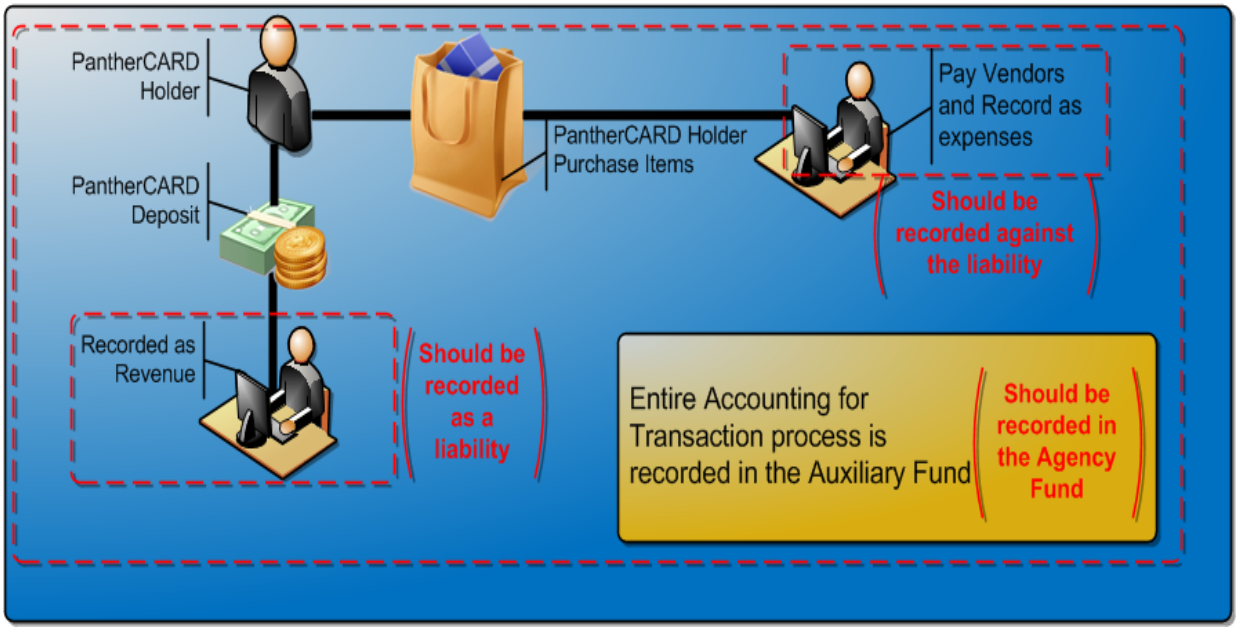
INTERNAL CONTROLS RATING FOR FINANCIAL CONTROLS			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		**x**	
Policy & Procedures Compliance		**x**	
Effect		**x**	
External Risk (to cardholders)		**x**	

INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls	**Effective**	**Opportunities exist to improve effectiveness**	**Do not exist or are not reliable**
Policy & Procedures Compliance	**Non-compliance issues are minor**	**Non-Compliance Issues may be systemic**	**Non- compliance issues are pervasive, significant, or have severe consequences**
Effect	**Not likely to impact operations or program outcomes**	**Impact on outcomes contained**	**Negative impact on outcomes**
External Risk	**None or low**	**Potential for damage**	**Severe risk of damage**

1. Accounting and Financial Reporting

PantherCARD financial transactions are being recorded as revenues and expenditures instead of liability accounts. In addition, these transactions were recorded in the Auxiliary Trust Fund instead of the Agency Trust Fund.

The Controller's Office has been recording cardholder deposits as revenues ($4,516,029). When the funds were used to pay vendors for the cardholders' purchases of goods and services, the PantherCARD Office processed these transactions as expenses ($4,236,084). Based on our interpretation of Generally Accepted Accounting Principles, deposits and drawdowns of cardholder funds by PantherCARD users should be recorded in a liability



account. We previously reported this during our last audit (Report No. 94/95-190, "*Debit Card Plan*," issued May 31, 1995).

During our audit fieldwork, in March 2011, the Controller's Office adjusted the University's general ledger to reflect the balances in the Plan accounts by adjusting the deposits payable account. Adjustments were being made manually on a monthly basis, until such time as the accounts were re-coded in April 2011. According to the Controller's Office a prior period adjustment to the financial statements will not be necessary.

However, in discussions with PantherCARD Office personnel, we identified that at any month's end, the balance in the Plan accounts excluded the amounts payable to the various vendors, including University departments, for purchases made by the cardholders. The University's general ledger is not capturing this liability. (See also Finding No. 6, for liabilities related to cardholder refunds). At our request, PantherCARD Office personnel provided us with a vendor liability schedule as of December 31, 2010. The schedule reflected a balance due vendors of $590,926, including $409,954 to other University departments.

While most individual account balances reflected one to three months of activity, the FIU Cashiers account was owed $348,124; reflecting more than 4 years of activity. Our review of the University's accounting records as of December 31, 2010, revealed that the FIU Cashier's accounts did not reflect a corresponding receivable for the $348,124. The Controller's Office

has informed us that this balance represents student tuition payments via the PantherCARD, and that when the employee in Student Financials separated from the University in April 2009 he was "behind" in processing these transactions. Upon his departure these responsibilities were not reassigned. We also found a $14,028 un-reconciled discrepancy between the amounts due to/from the Office of Business Services and the PantherCARD Office.

In addition, these cardholder deposits and vendor payment transactions were recorded in the University's Auxiliary Trust Fund instead of the Agency Trust Fund. Auxiliary funds are established to account for the operations of self-supporting enterprises; they exist primarily to furnish services to students, faculty and staff. The University, in receiving the cardholder deposits is solely acting as a custodian of the funds. Thus, the activity in the PantherCARD program should be recorded in the Agency Trust Fund. This finding was also identified in our Report No. 94/95-190, "*Debit Card Plan*," issued May 31, 1995.

Recommendations:

The Controller's Office should:	
1.1	Investigate and address the causes for the differences in the general ledger with the Cashier's Office and Office of Business Services.
1.2	Account for the PantherCARD activity in the Agency Trust Fund.

Management Response/Action Plan:

1.1 The Controller's Office has created a process whereby it will begin working with the Office of Business Services to reconcile the FIU One Card activity in the General Ledger on a monthly basis

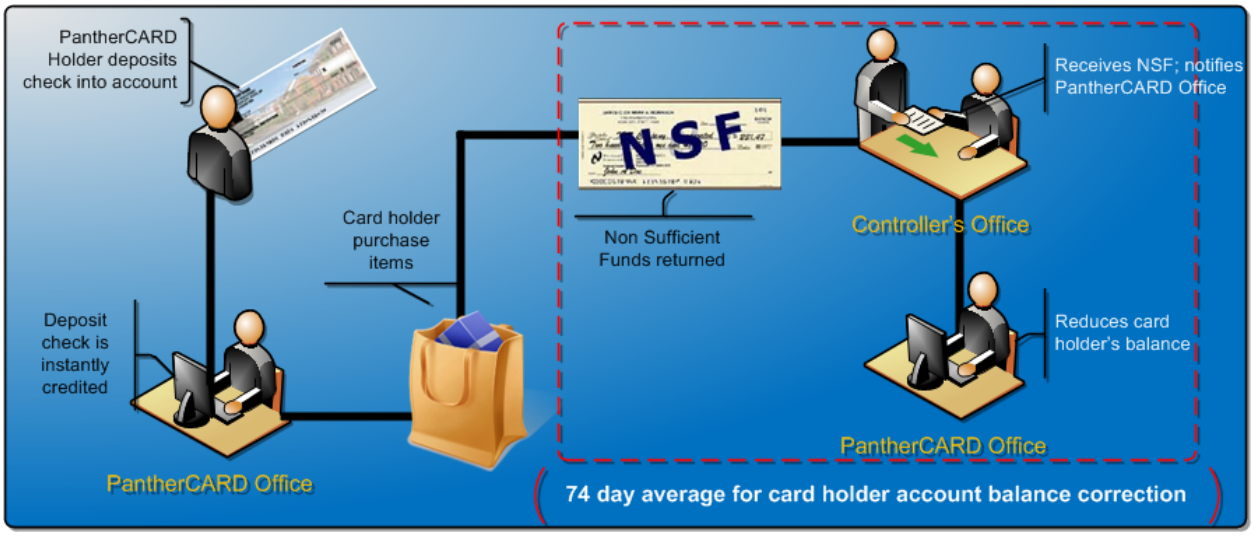
Implementation date: October 31, 2011

1.2 The change will be made for the fiscal year beginning July 1, 2011.

Implementation date: September 30, 2011

2. Returned Checks

The PantherCARD Office accepts cash, check, or money order for deposits. Under the current practice, account holders are to have immediate access via PantherCARD to their funds once they make a deposit to their account. This exposes the University to the risk of loss for amounts the cardholder spends when the check they deposited is returned for insufficient funds. The PantherCARD Office is not timely notified by the Controller's Office of checks being returned by the bank for insufficient funds.



Our review of the account plan balances revealed 41 PantherCARD holders with negative balances, totaling close to $9,400, resulting mostly from returned checks. Of the 41 cardholders, 40 were or had been active students. Three were currently enrolled and active in the semester ($4,261) and the other 37 had either graduated or were active but were not currently enrolled ($5,121).

We tested 18 of the 41 balances. Seventeen balances had resulted from returned checks, ranging from $50 to $4,000. The time elapsed from when the cardholders' deposited the bad checks to when the PantherCARD Office withdrew the funds from the cardholders' account averaged 74 days, ranging from 15 to 482 days. Of the 18 student-cardholders tested, 11 did not have PantherCARD related holds placed on their accounts, which would prevent them from conducting business with the University until the balance was paid off. In our Report No. 94/95-190, "Debit Card Plan," issued May 31, 1995, we recommended that the PantherCARD Office "…explore alternatives with the Controller's Office to reduce the time it takes . . . to be notified of a retuned check."

Another layer of control available, as a stop-loss measure, is to set PantherCARD CS Gold system minimum and maximum limits to appropriate levels. We evaluated whether established PantherCARD limits were set and were an effective triggering mechanism to alert administrators. We noted that the maximum limits were set at $9,999 and $999,999.99 for book advance and generic PantherCARD plans, respectively. In its present configuration, maximum thresholds are currently set at the system's maximum limit and thus, are not being used. The maximum threshold could effectively be used by management for different purposes, including ensuring funds from cardholder deposits exceeding the threshold are actually available prior to allowing access to funds; setting limits on the amount of funds to be allowed in the account; and

reporting requirements for cardholder deposits potentially exceeding Bank Secrecy Act and IRS guidelines.

Minimum balance trigger mechanisms, including low balances, alerts PantherCARD users at the time of purchase when their card balance is within the low balance range. Purchase transactions are properly denied when the minimum balance is exceeded.

Recommendations:

The PantherCARD Office should:	
2.1	Review its policies regarding the immediate availability of funds to cardholders for checks, especially foreign checks, and consider implementing a check verification process.
2.2	Ensure that student cardholders have a hold placed on their Student Financials account if they have a negative balance.
2.3	Evaluate whether the system's maximum thresholds should be used to provide management with additional controls.

Management Response/Action Plan:

2.1 The FIU One Card Office reviewed the policies regarding immediate availability of funds to cardholders and made the following adjustments:
The following types of deposits are immediately available after deposit:

1. Cash deposited at a ValuePort machine on any FIU Campus, or in person at the FIU One Card Office.
2. Electronic payments made using the FIU One Card NetCardManager portal.
3. U.S. Postal Service money orders deposited in person at the FIU One Card Office.
4. Cashier's, certified, or teller's checks deposited in person at the FIU One Card Office.

International checks are not accepted.

Finalization of the procedures for handling local and non-local checks is ongoing and will be completed by August 22nd.

The Finance Team within the Office of Business Services will periodically audit operating procedures within the ID office to ensure compliance. This final procedure will be outlined in the newly created employee handbook.

Implementation date: August 22, 2011

2.2 As part of the re-organization of the FIU One Card Office, the Office of Business Services is working with the FIU Student Financials to create a negative service indicator to be placed on a student's Student Financials Account in the event of a negative balance.

Implementation date: September 30, 2011

2.3 The FIU One Card Office evaluated whether the system's maximum thresholds should be used by management, including ensuring funds from cardholder deposits exceeding the threshold are actually available prior to allowing access to funds, and has determined that they are not necessary. The FIU One card is a debit account and as such does not allow students to spend dollars beyond what is available. Therefore, a maximum threshold is not necessary.

Implementation date: Immediately

3. Vendor Payments

Overall, the established internal controls over vendor payments were good.

The PantherCARD Office receives monthly statements from University vendors for transactions made using the PantherCARD. The PantherCARD Office reconciles those statements to their internal records prior to issuing payments to the vendors.

We sampled 18 disbursements totaling $2,334,347, representing 55% of all disbursements made, and noted the following:

- Two invoices, totaling $1,485,780, were miscoded as medical supplies.
- Vendor invoices are reconciled via a spreadsheet that is updated daily with cardholder vendor transactions. There was no apparent benefit to the daily updates.

During our audit, we also found two payment transactions for $3,134 and $3,033, paid in September 2010 for amounts due a vendor in 2008. Management explained that the vendor had not invoiced the University and only did so when requested. We were also informed that no contracts existed with vendors for the use of PantherCARD. When a PantherCARD holder uses their card to make a purchase transaction an obligation is created to pay the vendor using the cardholder's funds. Large past due liabilities currently have accumulated, mainly as a result of vendors not invoicing the PantherCARD Office. There appears to be no valid reason to wait until the receipt of an invoice from the vendor to make payment. PantherCARD Office personnel informed us that in most, if not all cases, the reconciliation currently performed with the vendor's invoice simply corroborates the system's totals.

Recommendations:

The PantherCARD Office should:	
3.1	Strengthen the current review processes to ensure that all transactions are properly coded.
3.2	Streamline the monthly vendor reconciliation and payment process.

Management Response/Action Plan:

3.1 As part of the re-organization of the FIU One Card Office, the roles and responsibilities of office staff have shifted. The Office of Business Services will be responsible for verifying and reviewing transactions and related coding. The Finance Team within the Office of Business Services will periodically audit operating procedures within the ID Office to ensure compliance. This procedure will be outlined in the newly created employee handbook.

Implementation date: August 22, 2011

3.2 As part of the re-organization of the FIU One Card Office, the roles and responsibilities of office staff have changed. The Finance team within the Office of Business Services will be responsible for monthly vendor reconciliation and processing related payments. The Finance Department will also be responsible for reconciliation of vendor payments and will periodically audit operating procedures within the ID Office to ensure compliance. This procedure will be outlined in the newly created employee handbook.

Implementation date: August 22, 2011

4. Copy Cards

Controls over copy cards are good, as copy cards are handled similarly to the PantherCARD.

As noted in the Background section, there were approximately 117,000 copy cards used for Business Services with a balance of $134,300 at December 31, 2010. Unlike the PantherCARD, copy cards require minimal formality in acquiring and or adding funds and the identity of purchasers is unknown. To obtain or add funds to the PantherCARD an individual must complete forms and abide by certain terms and conditions. The copy card is purchased through a vending type machine and has no terms and conditions. Yet the copy card provides individuals with the same ability to purchase items as the PantherCARD thereby circumventing the procedures put in place for the use of the PantherCARD.

Recommendation:

The PantherCARD Office should:	
4.1	Place limitations on the use of the copy cards as originally intended and include it as separate plan.

Management Response/Action Plan:

4.1 As part of the re-organization of the FIU One Card Office, limitations have been placed on the copy cards to restrict their use to on campus duplicating functions. Copy cards have also been converted to Plan 315 to separate charges from debit account Plan 31.

Implementation date: Immediately

5. Dormant PantherCARDs

We found that there were a significant number of dormant PantherCARD balances according to a report that details the last date that cards were used and their respective balances. According to the "Last Used" report as of April 6, 2011, the Plan balance was $1,541,894, excluding copy cards. Over 50% of the PantherCARD balances, or $809,000, were on cards not used in over a year.

The following table reflects the aging of the PantherCARD balances as of April 6, 2011:

Aging	Balance	Percentage
Less than 1 year	$732,107	47.5%
1 to 3 years	293,079	19.0%
3 to 5 years	152,031	9.9%
5 to 7 years	126,492	8.2%
Over 7 years	238,185	15.4%
Total	**$1,541,894**	**100.0%**

Under the terms and conditions signed by the cardholders in their Debit Account Application: "The agreement expires upon graduation, formal withdrawal from the University, or formal withdrawal from the Debit Program. Any balance remaining in the account at the expiration of this agreement will be refunded upon request. . ." The agreement also stipulates that "Future changes in terms and conditions regulating use of this card will apply to all cards in circulation and use at that time and will supersede the terms and conditions in effect at the time the card was acquired."

There is a State statute covering unclaimed funds, Florida Statute 717.113, which according to the General Counsel's Office, "appears to apply to state universities" as a public body corporate. However, the General Counsel's Office was continuing to research this matter at the time of this report as there appear to be other scenarios in which such funds may not need to be declared unclaimed.

Recommendations:

The PantherCARD Office should:	
5.1	Identify student cardholders that have graduated from the University or formally withdrawn, or employees who have separated from the University and obtain guidance from the General Counsel's Office on determining which funds, if any, need to be declared unclaimed for State remittance purposes.
5.2	Review current practices and consider implementing procedures to ensure that future student cardholders receive immediate refunds upon graduation or formal withdrawal from the University.

Management Response/Action Plan:

5.1 As part of the re-organization of the FIU One Card Office, accounts without activity (i.e., transactions or deposits) for two semesters, excluding summer terms or military withdrawals, will be classified by the FIU One Card Office as dormant accounts in accordance to University policies and standards.

A file will be generated from PantherSoft to determine when a student or employee is no longer affiliated to the University. The new procedure will provide the ability to automate the refund process and report the account balance owed to the patron.

The Office of Business Services is working with the General Counsel's Office to determine a feasible solution to address the fund balance. This is a unique and complicated challenge that warrants detailed review. A procedure will be put in place by September 30, 2011.

Implementation date: September 30, 2011

5.2 The Office of Business Services is working with the General Counsel's Office to determine a feasible solution to this recommendation. This is a unique and complicated challenge that warrants detailed review. A procedure will be put in place by September 30, 2011.

Implementation date: September 30, 2011

6. Cardholder Refunds

During our audit period there was a total of $518,000 in cardholder refunds. We judgmentally selected 25 refunds, totaling $12,750, to test their propriety. The PantherCARD Debit Account Terms and Regulations provide that "all refund checks must be mailed within 30 days of receipt" of the refund request. However, 10 of the 25 sampled refunds (40%) were paid more than 30 days after the refund request, ranging from 31 to 139 days.

Once the refund paperwork request is completed, the Associate Director is required to approve the request prior to it being sent to the Controller's Office for payment processing. However, on average, the approval took place 14 business days after the cardholder refund request. One transaction was not approved until 57 business days later.

Procedures also require closing out the account (zeroing out the balance on CS Gold) at the time of the cardholder refund request in order "to secure the funds from time of request to time of posting." While all the refunds tested were for the correct amount, in 9 instances (36%) the account closeout occurred between 3 to 54 business days after the request was received.

In addition, we noted that refund requests processed in CS Gold but not yet paid out by the Controller's Office at December 31, 2010 totaled $9,495, and were not reflected as a liability at year end on the University's financial statements. Subsequent changes to how financial obligations were captured by the Controller's Office to adjust financial statements did not capture this liability at March or April 2011.

Recommendation:

PantherCARD Office should:	
6.1	Ensure that PantherCARD refunds are processed within the required 30-day timeframe.

Management Response/Action Plan:

6.1 As part of the re-organization of the FIU One Card Office, an internal procedure is being created for the processing of refunds to include details for submitting refund requests to the FIU Office of Student Financials. Additionally, as the roles and responsibilities of office staff have shifted, the Cashier in the FIU One Card Office will be specifically responsible for coordinating refunds with the FIU Office of Student Financials. This procedure will be outlined in the newly created employee handbook.

All approved withdrawals/refunds will be transmitted to the cardholder by the Office of Student Financials in accordance with their policies and procedures.

Implementation date: August 22, 2011

7. Cardholder Deposits

We sampled 56 cardholder deposits, totaling $20,633, to ensure that the controls in place align with University policies and procedures. The following exceptions were noted:

- Deposit transactions are supposed to be input into PantherSoft on a daily basis by the Program Assistant. However, in her absence transactions are not input until her return since there are no backup personnel designated to post these transactions in her absence. For 18 of the sampled transactions there was a 2 to 14 day delay between the time the cardholder deposited the funds into their account and the time that information was posted to PantherSoft.

- While current procedures require funds to be immediately made available to the cardholder, there were six transactions in which there was between a 1 to 13 day delay in posting to CS Gold, resulting in the cardholder not having access to those funds during that period.

- For 17 transactions there was a delay of more than four business days from the time of the cardholders' deposit to the time the monies were posted by the bank. The delay ranged from 5 to 16 days. University Policy 1110.010, *Cash Control Policy Statement*, states that bank deposits should be deposited daily, especially since pre-numbered receipts and records are not used.

- For 53 of the 56 sampled transactions the cashier on duty did not initial the Debit Account Deposit form as required, resulting in a loss of accountability. In addition, since cardholders deposit funds using the PantherCARD Debit Account Application form, such forms should likewise require the cashier's initials.

- Four employees in the PantherCARD Office act in the cashiering capacity, three of whom are student employees. None of the four employees have had a background check as required by University Policy.

- A fifth employee, who collects cash when no one else is available, is responsible for performing the monthly reconciliations, which is an improper segregation of duties.

Recommendations:

PantherCARD Office should:	
7.1	Appoint an alternate employee for inputting deposits into PantherSoft in the primary employee's absence.
7.2	Ensure that monies deposited by cardholders are available more promptly, except in the circumstances where the PantherCARD Office has not been able to verify availability of funds (e.g., foreign checks or unverified domestic checks).
7.3	Deposit all monies at the bank daily.
7.4	Ensure that all deposit forms provide for and include the cashier's initials.
7.5	Work with Human Resources to ensure that all employees who handle cash, whether physically or through electronic means have had requisite criminal background and/or fingerprint checks performed.
7.6	Appoint an alternate employee, not assigned to collecting cash, to perform monthly reconciliations.

Management Response/Action Plan:

7.1 As part of the re-organization of the FIU One Card Office, an alternate employee for inputting deposits into PantherSoft has been designated. The primary employee entering deposits into PantherSoft and handling cash transactions will be the Cashier in the FIU One Card Office. The Office Manager will be an alternate employee for inputting deposits. The Office of Business Services will reconcile journal entries in PantherSoft and manage deposit verification against CS Gold.

The Finance Team within the Office of Business Services will periodically audit operating procedures within the ID Office to ensure compliance. This procedure will be outlined in the newly created employee handbook.

Implementation date: August 22, 2011

7.2 The FIU One Card Office reviewed the policies regarding immediate availability of funds to cardholders and made the following adjustments:

The following types of deposits are immediately available after deposit:

1. Cash deposited at a ValuePort machine on any FIU Campus, or in person at the FIU One Card Office.
2. Electronic payments made using the FIU One Card NetCardManager portal.
3. U.S. Postal Service money orders deposited in person at the FIU One Card Office.
4. Cashier's, certified, or teller's checks deposited in person at the FIU One Card Office.

Funds from local checks will be made available once the University Cashier's Office has confirmed to the FIU One Card Office that the funds have cleared.

Funds from non-local checks will be made available once the University Cashier's Office has confirmed to the FIU One Card Office that the funds have cleared.

International checks will not be accepted.

Finalization of the procedures for receiving notification of cleared checks from the cashier's office is ongoing and will be completed by August 22nd. The FIU One Card Office is also still evaluating the possibility of implementing a check verification procedure; a final determination of this procedure will be made by August 22, 2011. This final procedure will be outlined in the newly created employee handbook.

Implementation date: August 22, 2011

7.3 As part of the re-organization of the FIU One Card Office, the Office of Business Services will be entering into an agreement with Brink's, Incorporated for the daily pick-up and deposit of all funds collected by the FIU One Card Office and the ValuePorts located across campuses.

The Finance Team within the Office of Business Services will periodically audit operating procedures within the ID Office to ensure compliance. This procedure will be outlined in the newly created employee handbook.

Implementation date: August 22, 2011

7.4 As part of the re-organization of the FIU One Card Office, an internal procedure is being created regarding deposits, including the initialing of all deposit forms. This procedure will be outlined in the newly created employee handbook.

Implementation date: August 22, 2011

7.5 As part of the re-organization of the FIU One Card Office, the Office of Business Services confirmed that all employees of the FIU One Card Office have completed the requisite background and/or fingerprint checks performed. All future employees of the FIU One Card Office will undergo similar screening and will be documented by the Assistant Director of the FIU One Card Office. This procedure has been outlined in the newly created employee handbook.

Implementation date: Immediately

7.6 As part of the re-organization of the FIU One Card Office, an alternate employee for inputting deposits into PantherSoft has been designated. The primary employee entering deposits into PantherSoft and handling cash transactions will be the Cashier in the FIU One Card Office. The Office Manager will be an alternate employee for inputting deposits. The Office of Business Services will reconcile journal entries in PantherSoft and manage deposit verification against CS Gold.

The Finance Team within the Office of Business Services will periodically audit operating procedures within the ID Office to ensure compliance. This procedure will be outlined in the newly created employee handbook.

Implementation date: August 22, 2011

8. Access to Student Banking Data

During our audit we observed that cardholder refunds were mostly paid via electronic bank transfers. These transfers were sent to student-cardholders who had set up their banking information online. A review of information systems access controls over sensitive banking data found 19 individuals within the University which could not only view the data since the fields were not grayed out, but with access privileges to write/edit student bank account and bank routing numbers. Included were 14 individuals whose duties and responsibilities were not related to Student Financials.

Twelve of the 19 employees with access to such data fields had not had criminal background and/or fingerprint checks, as required under various University policies in effect since 1990.

Lastly, we noted that no audit trail was available for changes made to these fields. An audit trail, which is reviewed by management routinely, would provide management with the ability to track who made the changes and enable them to more easily and timely detect any changes deemed inappropriate.

Recommendations:

The Controller's Office should:	
8.1	Restrict access, including write/edit privileges; to those individuals who require access to Student Banking information as part of their regularly assigned duties.
8.2	Work with Human Resources to ensure that all employees who handle cash, whether physically or through electronic means have had requisite criminal background and/or fingerprint checks performed. (Same as Recommendation 7.5)
8.3	Enable and periodically review audit trails for changes to Student Banking data fields.
Division of Information Technology should:	
8.4	Ensure that Roles and Permissions providing access to such sensitive data fields are hidden or grayed out.

Management Response/Action Plan:

8.1 The Controller's Office has restricted access of FIU employees to view cardholder's banking data and/or privileges to write/edit cardholder's bank account and bank routing numbers.

Implementation date: Immediately

8.2 The Controller's Office will work with the Office of Human Resources to identify any new employees with cash handling responsibilities so that Human Resources may perform the requisite background and/or fingerprint checks. As previously advised by the Controller's Office, the Controller's Office has no direct role in HR policy or background check practices.

Implementation date: Immediately

8.3 The Controller's Office is working with the PantherSoft UTS team to develop an audit trail.

Implementation date: December 31, 2011

8.4 PantherSoft has removed access to the student banking (Direct Deposit) information page from all non-Student Financials support personnel with the exception of three database administrators. There are currently three Student Financials resources supporting the application and need the access to support students with issues or problems pertaining to their direct deposit. The access maintained for the three database administrators is for full application support of the database and application.

Implementation date: Immediately

9. Contractual Agreements

During our audit we requested copies of contracts with vendors to determine duties and responsibilities of the parties as it related to PantherCARDs. Management informed us that except for one contract currently in place with vendors accepting PantherCARDs, the remaining contracts do not address PantherCARD processing.

Formalizing the relationship between the vendors and the PantherCARD Office would mitigate any issues that may arise from a misunderstanding, disagreement, or a simple difference, e.g., Finding No. 3 addressed the fact that vendors do not get paid unless they provide the PantherCARD Office with an invoice. However, with nothing in writing to that effect, and an obligation having been created, if the vendor had not or could not provide an invoice the PantherCARD Office would be in a difficult position. In addition, if any differences existed in the amounts owed to vendors there is no formal process to resolve those differences.

Recommendation:

The PantherCARD Office should:	
9.1	Enter into formalized agreements with vendors accepting PantherCARDs to address each party's duties and responsibilities and conflict resolution processes.

Management Response/Action Plan:

9.1 The FIU One Card Office will supplement agreements with existing vendors that accept the FIU One Card and will draft addenda, as necessary, regarding each party's duties and responsibilities and conflict resolution processes.

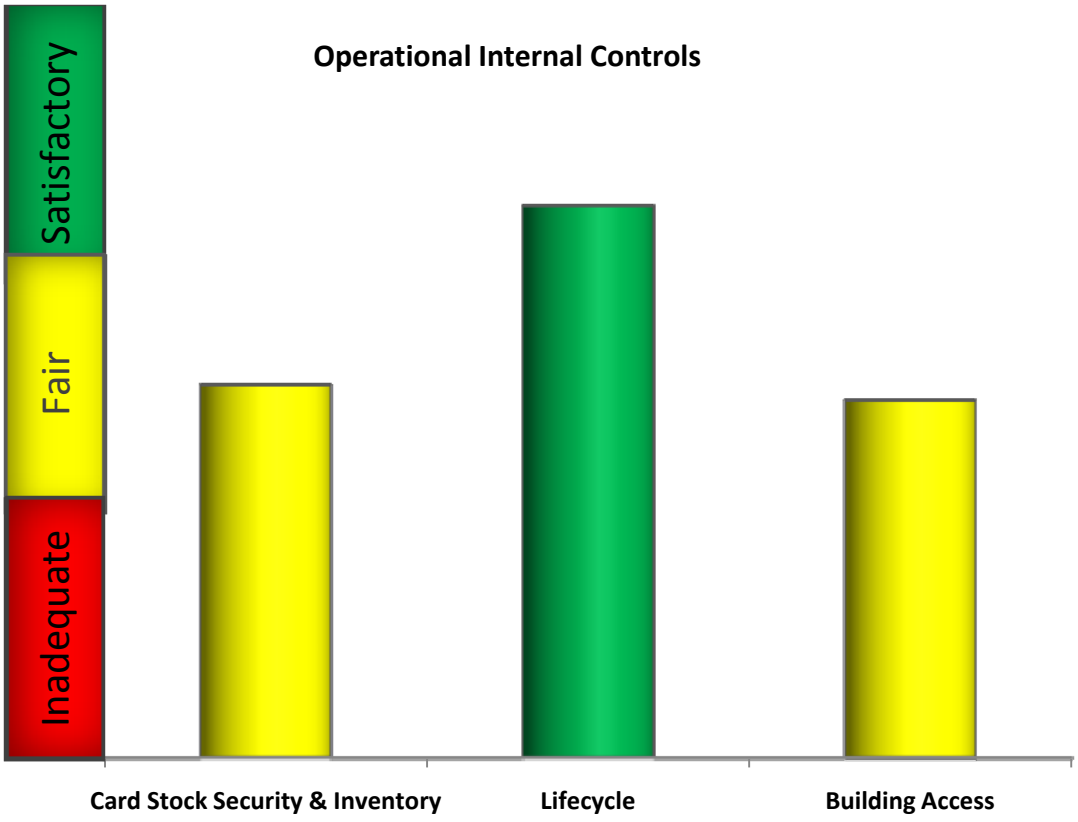
Implementation date: April 30, 2012

Operational Controls

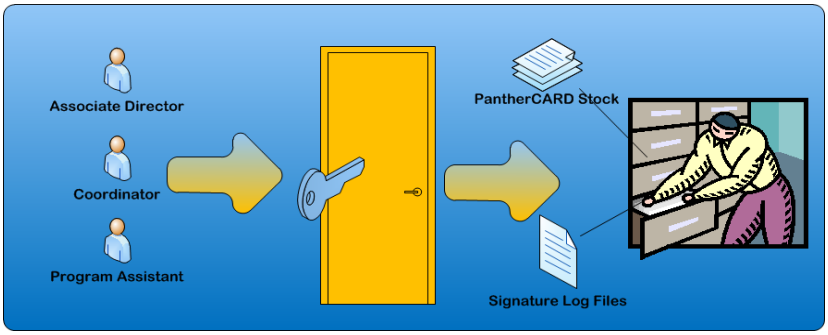
We focused our audit of Operational Controls on card stock physical security and inventory, card lifecycle, from creation to deactivation, and the cards use for building access. With the exception of card lifecycle processes, the operational controls over PantherCARDs identified areas in need of improvement, particularly in the use of temporary PantherCARDs; the need for electronic backup of inventory logs; and the accessibility to the Inventory Log File.

With regard to the use of the PantherCARDs to control access to certain buildings, floors, and rooms during and after working hours, controls are in place that assure identification of actual card use for that purpose. However, how card access is assigned and later withdrawn, which is critically important, needs improvement.

Our overall evaluation of internal controls for PantherCARD Operational Controls is depicted in the chart below.



10. Card Stock Security & Inventory



Physical security over unused PantherCARD stock is good. The PantherCARD storage room was closed and locked when not in use. PantherCARD stock and signature log files are securely stored in a locked storage room. The storage room is accessible only via key access. Access to the storage room is appropriately limited to the Associate Director, Coordinator, & Program Assistant.

PantherCARD stock is separately located in a file cabinet appropriately segregated from other storage room items, which is an effective physical security control.

The PantherCARD Office tracks and maintains their inventory orders of unused PantherCARD stock on an electronic spreadsheet. Card boxes received are recorded on the spreadsheet and kept in reserve until needed. Orders for additional PantherCARDs are placed as reserves fall below 3,000. We noted that due to an inventory shortage, between August 23, 2010 and August 27th 2010 the PantherCARD Office issued blank temporary cards to 1,929 students and faculty members. According to the Coordinator, students and faculty members who received the temporary cards were directed to stop back the following week to obtain their official PantherCARDs. In addition, vendors were notified either verbally or over the phone to accept the temporary cards. The PantherCARD Office did not formally notify students and faculty members to return the temporary cards nor were these cards disabled. We concluded that the continued active use of the temporary cards may cause confusion with management and vendors as to whether the cards are legitimate, active and authentic and should be discontinued.

PantherCARD holders are required to sign a “hard copy” card file log as proof of receipt at time of issuance. We noted that there is only an original copy of the card log stored in the inventory room. A backup copy would ensure that the log files would be still be available in the event they was destroyed due to theft, negligence, or disaster.

The PantherCARD Inventory Log File is located on a network shared folder and is reviewed routinely by three PantherCARD employees (Associate Director of Multipurpose Facilities, Coordinator of Administrative Services, and Program Assistant) as part of their job duties. An effort has been made by the PantherCARD Office to limit user access through the creation of user groups. We noted, however, that the inventory log is accessible to an additional seven (7) user accounts, three (3) administrator group accounts, and four (4) administrator user accounts.

Recommendations:

The PantherCARD Office should:	
10.1	Locate and reissue standard PantherCARDs to remaining temporary card holders.
10.2	Maintain a backup of the Inventory Log.
10.3	Limit user account access to a network shared folder where the Inventory Log File is located.

Management Response/Action Plan:

10.1 A file will be created to identify all cards previously issued as FIU Emergency Cards and a notification will be sent to all cardholders of future expiration of the card and how to receive their new FIU One Card.

Implementation date: September 30, 2011

10.2 As part of the re-organization of the FIU One Card Office, all Inventory Logs will be stored electronically on the CS Gold System. This procedure will be outlined in the newly created employee handbook. The CS Gold System maintains all records from 2003 to date where authorized users could retrieve record files at any time. The FIU One Card Office will no longer issue paper logs to maintain inventory; instead, there will be an automated report available on CS Gold.

Implementation date: August 22, 2011

10.3 As part of the re-organization of the FIU One Card Office, the Card Stock Inventory Logs will be stored electronically on the CS Gold System, and user access will be limited to authorized users (see also, response to No.10.2).

Implementation date: August 22, 2011

11. PantherCARD Lifecycle

The PantherCARD Office has good internal identification card policies that document the authorization and identification process for both Student and Faculty/Staff. The policies adequately address authorization and card issuance requirements. The PantherCARD Office adequately defines new and replacement card access procedures in the Student and Faculty/ Staff Identification Card policies. It would be useful to post these policies on the University's policies website.

The identification card eligibility requirement for faculty and staff states that the individual must be a current FIU employee; students must be currently enrolled. Additionally, PantherCARD Debit Cardholder agreements are signed by eligible users upon account creation. PantherCARD eligibility requirements are adequately defined in the Identification Card Policy and Debit Account Applications. Though there should be a backup process for signed Debit Account Applications.

We sampled 50 terminated user accounts and verified that all the Faculty/Staff and OPS selections were properly deactivated within the CS Gold system.

Recommendations:

The PantherCARD Office should:	
11.1	Add internal identification card policies to the University's policies website.
11.2	Maintain an electronic backup for signed Debit Account Applications.

Management Response/Action Plan:

11.1 As part of the re-organization of the FIU One Card Office, all policies for the FIU One Card Office, including policies relating to the issuance of internal identification cards, will be posted on the University Compliance Office's Policies and Procedures Website. An internal handbook will also be distributed to all FIU One Card Office employees.

Implementation date: September 30, 2011

11.2 As part of the re-organization of the FIU One Card Office, FIU One Card Debit Accounts will be automatically issued to all cardholders; the office will no longer collect debit account applications. All cardholder's signatures are captured and stored in CS Gold.

Implementation date: Immediately

12. PantherCARD Building Access

For security purposes, the University uses PantherCARDs to control access to certain buildings, floors, and rooms during and after working hours. The PantherCARD is used by University employees to gain entry into buildings and rooms throughout the University. The FIU Procedure 520.005a states that the Facilities Management Department should be the central control point for the issuance, maintenance, and secured storage of all types of software, hardware and access mechanisms used on interior and exterior doorways for all campus buildings and facilities. Additionally, COBIT DS12.2 states that physical security measures should be in line with business requirements to secure the location and the physical assets.

The Key Control Office in Facilities Management is accountable for ensuring that specific access is activated based on proper authorization by the requesting department and deactivated upon employee separation or change in assignment. Currently, Key Control is delegating the responsibility of building access privileges to specific colleges and departments to improve request completion times.

Key Control requires requesting departments to provide employee's username and Panther ID to activate and provide access. We randomly sampled 25 emails from requesting departments and found all to contain the username and Panther ID.

Eighteen delegated colleges and departments can perform PantherCARD building access but are required to sign off on that Key Control's Acceptable Use Procedure to ensure their understanding of the responsibilities that go along with performing this function independent of Key Control. However, twelve of the colleges or departments which were delegated the ability to perform PantherCARD building access had not signed the Form.

We reviewed building access authorizations, which were handled by Key Control, the College of Business Administration, and the College of Medicine. The ten access requests handled by Key Control and the College of Medicine had the username, Panther ID, and location(s). The College of Business Administration did not adequately document PantherCARD building access, which may reduce the effectiveness of existing building access controls. The two building requests handled by the College of Business Administration were: (1) missing a specific location; and (2) was said to be handled in person and thus, no supporting documentation was retained.

The existing procedures for PantherCARD building access revocation to premises, buildings, and areas are inadequate and ineffective in revoking physical access in a timely and accurate manner. Key Control should define and implement procedures to revoke building access in a timely manner. We found:

- 15 terminated users still had active building badge access, an average of 340 days after termination.
    - Four had their separation agreement form filled out in a timely manner, however, they were still listed as active, an average of 347 days after termination.
    - The remaining 11 terminated employees were still active, on average, 338 days after termination.
- College of Medicine's former Director of University Computer Systems was still listed with active building access to 20 separate rooms in 4 separate locations.

Key Control personnel states that they rely on receiving the University's separation clearance form from Human Resources in order to remove access from separated employees. Department heads are to complete the form and submit it to Human Resources upon an employee's separation. According to Key Control, they receive very few of these forms, and as a result, timely deactivation does not occur.

In conclusion, the physical access control aspect of the PantherCARD adequately identifies the card used to gain access to either a specific restricted area or afterhour's access. However, how card access is assigned and later withdrawn, which is critically important, needs improvement.

Recommendations:

The Key Control Department should:	
12.1	Ensure that delegated colleges follow the required process.
12.2	Require delegated colleges and departments to sign the Key Control Acceptable Use Procedure statement.
12.3	Ensure delegates perform acceptable access provisioning and de-provisioning procedures by adequately documenting delegated roles and responsibilities within the Key Control Acceptable Use Procedure document.
12.4	Work with Human Resources to implement procedures to revoke PantherCARD access to premises, buildings, and areas in a timely and accurate manner.

Management Response/Action Plan:

12.1 Key Control will monitor all system operators through quarterly audit reports. These reports will be generated by the SMS software and Key Control will initiate the system to produce the reports.

Implementation date: August 19, 2011

12.2 All operators will be required to sign the "Key Control Acceptable Use Procedure KC-1.0.1" annual form by August 19, 2011. The form must be renewed on an annual basis.

Implementation date: August 19, 2011

12.3 The "Key Control Acceptable Use Procedure KC-1.0.1" has been amended to describe the role of the system operator and responsibilities.

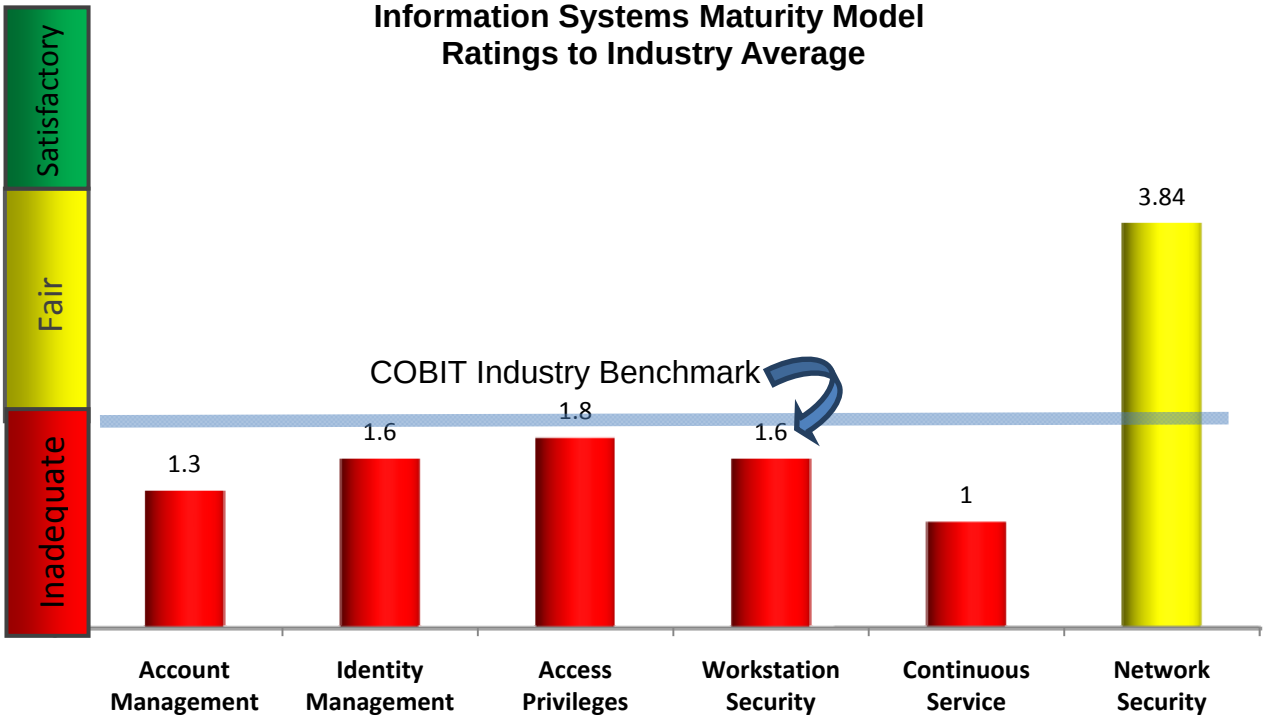
Implementation date: Immediately

12.4 Facilities Management Department is creating an electronic interface. The ID Office currently receives an electronic file from HR concerning personnel status. This new electronic transfer will be operational by November 2011. Until this becomes active we will continue to receive the file from the ID Office manually and make "add/delete" adjustments.

Implementation date: November 2011

Information Systems Controls

We focused our information systems audit on account management, identity management, access privileges, workstation security, continuous service, and network security. Based on Control Objectives for Information and related Technology (COBIT) benchmark data, five of the six controls fall below public sector averages.



COBIT's maturity modeling over IT processes is based on a method of evaluating existing processes in a measurable fashion. A maturity model has been defined for each of the COBIT IT processes, providing an incremental measurement scale from 0 to 5 as follows:

0 = Non-existent: Complete lack of any recognizable processes. The audited departments do not even recognize that there is an issue to be addressed.

1 = Initial/Ad Hoc: There is evidence that the audited department(s) has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.

2 = Repeatable but Intuitive: Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3 = Defined Process: Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.

4 = Managed and Measurable: Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 = Optimized: Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modeling with other enterprises. Processes are used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the audited department(s) quick to adapt.

The PantherCARD Office needs to develop and formally document access controls and procedures for CS Gold. It is not evident that user accounts were being properly managed. Temporary, terminated employees, and emergency accounts need better management.

We found that unnecessary application privileges were granted to individual and vendor accounts which resulted in providing greater privileges than needed for the individuals to perform their related job functions. A single user with excess application privileges could circumvent existing controls and perform a malevolent act. We also found deficiencies in workstation security, which could potentially allow the installation of malicious software thereby increasing the risk of data loss or network disruption.

The PantherCARD does not have a Business Continuity Plan. This could greatly impact the integrity of its data and also financially impact PantherCARD dependent student and faculty/staff services and activities.

In all material respects the Network Management Services department provides network security that adequately protects the PantherCARD system. We found that they use a layered security approach to secure PantherCARD data in motion, including:

- Intrusion Protection Systems
- Firewalls
- Virtual Private Network connection
- Daily reviews of the Intrusion Protection Systems and Firewalls.

Details follow:

13. User Account Management

The primary purpose of user account management is to ensure that system changes are only performed by authorized users; that user accounts are used for their intended purposes; and to disable user accounts when no longer necessary.

A. Policies and Procedures

Based on NIST AC-1.1(i)(ii)[2],the PantherCARD Office should develop policies and procedures for allowing access to the CS Gold application. They should address purpose, scope, roles and responsibilities, and legal and regulatory guidelines. Once polices are developed, they should be reviewed and updated with defined frequency.

The PantherCARD Office does not have a formally documented Access Control Policy. It does, however, utilize an informal access request procedure, requiring an emailed request, which provides details on the username, department, and Panther ID. When establishing user accounts, we found that the PantherCARD Office's access control procedures were not adequate or effective as noted by the following:

- Three of nine sampled user accounts had an access request email, but did not explicitly state the intended access privileges.

[2] National Institute of Standards & Technology Guidelines Special Publications 800-53A

- One access request email was sent 20 days after the user account was created, but included the user's access privileges.

- One employee had two separate user accounts.

Obtaining user access to the CS Gold application should be based on a valid authorization, along with the user's intended use. The Computer Operations Manager receives informal requests from either the Associate Director of Multipurpose Facilities or a designated Aramark employee. The lack of formal access control policies and procedures increases the risks associated with inappropriate user access. Additionally, these procedures should apply for all users, including administrators (privileged users), internal and external users, and for normal and emergency cases.

B. Deactivation of User Accounts

Using NIST AC-2.1(i) as a guideline, information system account managers should be notified when temporary and terminated accounts are no longer required, and ensure user accounts and their related privileges are removed appropriately. We noted that PantherCARD Office deactivation requests may happen face-to-face, by telephone, or by email. Deactivation notification documentation for our sample selection was not provided as requested.

We noted that the informal PantherCARD Office procedure is to deactivate the CS Gold user accounts when notified of employment separation. We found 10 of 11 inactive accounts were adequately deactivated. However, we did find one user account which was not deactivated and still had active privileges 1,434 days after separation. Due to the length of access deactivation lapse, we are concerned that the informal user account deactivation process does not adequately notify CS Gold account managers when accounts are no longer needed.

Additional layers of security should be put in place to mitigate the risk of terminated user accounts remaining on the CS Gold application. These can include user access policies which define account time periods for each type of account or automatically disable user accounts after a defined time period of inactivity.

Defining user access time periods for temporary and emergency accounts is an effective control to ensure that these accounts are terminated upon their stated expiration.

Automated mechanisms ensure user account policies are adhered to and user accounts are not left active for an indefinite period of time. The PantherCARD Office should use automated mechanisms to automatically disable inactive accounts once the PantherCARD Office defines the inactivity time period. We noted that the PantherCARD Office uses a "semi" automated process whereby the Computer Operations Manager periodically reviews the daily report for inactive accounts. Inactive accounts may be missed during the manual review process and may increase the risk of inappropriate access after separation, as previously noted. A more effective automated mechanism is to have the CS Gold application automatically disable inactive user accounts, which the CS Gold application does not presently perform.

C. User Account Audit Trail

User audit trails are an effective control in documenting user account actions. Using NIST AC-2(4).1(i) as a guideline, the CS Gold application should automatically provide an audit trail of user account creation, modification, disabling and termination actions. We observed that the CS Gold does provide the date the user account was created in the User Manager screen.

Additional user actions including modification, disabling, and termination actions are not available through CS Gold. Additionally, appropriate PantherCARD individuals should be notified, as required, of audit trail information. An example, due to its inherent risk, is to require notification when privileged user access level modification occurs. This level of notification will ensure appropriate individuals are alerted to modifications of high risk privileged user accounts, which the CS Gold application does not presently perform.

D. Privileged User Access

Role based access schemes for privileged users are an effective means to group user accounts in a consistent manner to ensure appropriate user account access. The PantherCARD Office has established and administered privileged user access in accordance with a role based scheme. Currently, the CS Gold application has two privileged role based user account groups.

Due to the high degree of inherent risk due of elevated privileges, the PantherCARD Office should track and monitor privileged role assignments. The PantherCARD Office informally tracks and monitors privileged role assignments through periodic updates and directives from management regarding user privileges to the CS Gold application. The lack of formal tracking and monitoring of privileged user assignments increases the risk of inappropriate privileged access.

Recommendations:

The PantherCARD Office should:	
13.1	Develop and formally document an access control policy and procedures for CS Gold with periodic review and updates.
13.2	Ensure all user access requests are based on a valid authorization and their intended application usage.
13.3	Define start and end time periods for temporary and emergency user accounts and notify managers when accounts are no longer required.
13.4	Define a time period after which inactive accounts are automatically disabled and work with the application vendor to develop a process to automatically disable inactive user accounts within the defined time period.
13.5	Work with the application vendor to develop audit trails for account modification, disabling, and termination actions and provide notifications to appropriate individuals.
13.6	Formally track and monitor privileged user assignments.

Management Response/Action Plan:

13.1 As part of the re-organization of the FIU One Card Office, access control policies and procedures will be incorporated into an internal handbook for the office. The FIU One Card Office will re-define user access roles within CS Gold, and limit the number of Gold Admin Users.

Implementation date: December 31, 2011

13.2 As part of the re-organization of the FIU One Card Office, access control policies and procedures (including justification for same) will be incorporated into an internal handbook for the office. In addition to the measures taken in response to No.13.1, the FIU One Card Office will develop a procedure for CS Gold user authorization which includes an authorization form that will record all privileges for account users on file.

Implementation date: December 31, 2011

13.3 As part of the re-organization of the FIU One Card Office, policies and procedures regarding the issuance of user accounts will be incorporated into an internal handbook for the office. This will include the development of an “end time” to be defined in CS Gold as a locked account.

Implementation date: December 31, 2011

13.4 The FIU One Card Office will work with CBORD to develop a mechanism to expire user accounts after 30-60 days of inactivity.

Implementation date: December 31, 2011

13.5 The FIU One Card Office will work with CBORD to develop audit trails for account modifications, disabling, and termination actions.

Implementation date: December 31, 2011

13.6 Currently, the FIU One Card Office can monitor all deposits, transactions and cards issued in CS Gold. The FIU One Card Office will work with CBORD to develop a log to track user assignments.

Implementation date: December 31, 2011

14. Identity Management

The purpose of identity management is to uniquely identify user accounts so that they can be appropriately managed on the network.

A. Establishing Username and Passwords

We noted that the CS Gold application has 33 unique user accounts, which authenticate through the use of passwords. However, the CS Gold user account naming process was not uniformly assigned; therefore it was difficult to trace usernames to employees. Storing their associated Panther ID within the CS Gold application would increase the ability to identify individual users.

The use of user account passwords is an effective means to authenticate and ensure that the user account is being used by the individual that the account was intended for. We also noted that a network super user account, with one username and password, is shared by the Computer Operations Manager, Senior Telecommunications Specialist and Graham Center Coordinator of Computer Operations. The continued sharing of the super user account greatly reduces the effectiveness of identity management.

B. User Group Appropriateness

According to NIST AC-2.1(i), user accounts, which are grouped by type, such as individual, group, system, job function, or user department is an effective control to identify user accounts and their related privileges. The PantherCARD Office has established 13 unique user groups within the CS Gold application, which can be used to identify each user account and their related privileges.

We selected nine user accounts and verified the accuracy of their placement into user groups. There was documentation for four of the nine tested that uniquely identified them on the network. Their placement into established CS Gold user groups was not evident. We also noted that the remaining five user accounts did not have documentation to identify them or their group membership. Based on the above, it is uncertain as to how the PantherCARD Office is managing user accounts and ensuring that user accounts are placed in the correct group membership category.

Recommendations:

The PantherCARD Office should:	
14.1	Use a standard naming process and store the associated Panther ID for all CS Gold user accounts.
14.2	Discontinue shared usage of network super user accounts.
14.3	Establish explicit membership conditions for each CS Gold application User Group.

Management Response/Action Plan:

14.1 As part of the re-organization of the FIU One Card Office, all new CS Gold new user accounts will be identified though the MyFIU account authentication.

Implementation date: Immediately

14.2 As part of the re-organization of the FIU One Card Office, users will no longer share network super user accounts. All new workstations operate on AD and are behind a firewall.

Implementation date: Immediately

14.3 As part of the re-organization of the FIU One Card Office, policies and procedures regarding membership conditions for user accounts will be incorporated into an internal handbook for the office. The FIU One Card Office will re-define user access roles within CS Gold.

Implementation date: August 22, 2011

15. Access Privileges

Limiting access privileges reduces the possibility for a single individual to compromise a critical process. To mitigate the risk associated with privileged access, The PantherCARD Office should apply the concept of least privilege access where only authorized users are allowed access which is necessary to accomplish their assigned tasks.

There were two separate vendor user accounts; two senior managers; a program assistant who also performs financial transactions; a Computer Operations Manager; and a senior telecommunications services representative that were granted privileged access. We define privileged user access as an information systems account that has "System Administrator," "Root," or "Super User" capabilities including the ability to create, modify, delete or otherwise view sensitive and or confidential data without oversight. Super user accounts on the PantherCARD information system should only be designated to system administration personnel. Based on their respective jobs and positions, these user accounts are not limited to PantherCARD information system personnel.

Using NIST AC-6.1 as our guideline, the CS Gold application should enable finer-grained allocation of user privileges to provide an additional data security layer of least privileged account access. A high level of inherent risk is present on create, change, and delete access privileges. The CS Gold application has nine access privilege selections available which include these capabilities. We reviewed seven user accounts and found all had the ability to create and change access privileges. Six of the seven sampled also had delete access privileges. Additionally, we found vendor accounts having the ability to create, change, and delete privileges; senior management, which normally approve accounts, also having the ability to create, change, and modify PantherCARD user data. Excessive granting of privileged access increases the likelihood that a single user can compromise a critical process.

The PantherCARD Office should prohibit privileged access to information systems by non-University users to minimize the inherent risk of super user accounts were they following NIST AC-6(6).1 guidelines. We found two separate vendor accounts with administrator access on the CS Gold application which increases the risk for a single non-University user's ability to compromise a critical process. Additionally, based on their respective jobs and positions, user accounts within the privileged user groups are not applied in a least privileged manner.

Identifying roles and responsibilities, through the use of multiple user groups that are focused on specific areas of access, should reduce the possibility of a single individual's ability to compromise a critical process. The CS Gold application has multiple user groups from which users can be assigned to. Currently, the application vendor is listed as the owner of all user groups and is also a listed user account in each group. Additionally, there are six user accounts with access to multiple user groups including an application administrator group. The six individual accounts' roles and responsibilities include application vendor, computer operations, senior telecommunications specialist, associate director of facilities, program assistant with financial collection responsibilities, and meal plan vendor. We found the assignment of these accounts do not provide least privileged access relevant to their respective jobs and positions.

Recommendations:

The PantherCARD Office should:	
15.1	Review privileged user groups to ensure: a) Access is limited to those individuals with documented need based on necessity to accomplish assigned tasks; b) Privileged users with create, delete privileges are appropriate to those who perform these actions as part of their normal job duties; c) Authorizations to CS Gold Super User accounts are limited to designated system administration personnel.
15.2	Limit the number of users who have the ability to create, modify, and delete user data.
15.3	Disable vendor user accounts from Super User groups.

Management Response/Action Plan:

15.1 As part of the re-organization of the FIU One Card Office, policies and procedures regarding membership conditions for privileged user accounts will be incorporated into an internal handbook for the office. The FIU One Card Office will re-define user access roles within CS Gold.

Implementation date: August 22, 2011

15.2 As part of the re-organization of the FIU One Card Office, policies and procedures regarding user privileges will be incorporated into an internal handbook for the office. Gold Administrators in CS Gold are limited to FIU One Card IT staff, necessary CBORD personnel and the Assistant Director of the FIU One Card Office.

Implementation date: August 22, 2011

15.3 As part of the re-organization of the FIU One Card Office, vendor accounts will be disabled from Super User groups. An online reporting tool will be available for vendors to use without requiring access to CS Gold User groups.

Implementation date: December 31, 2011

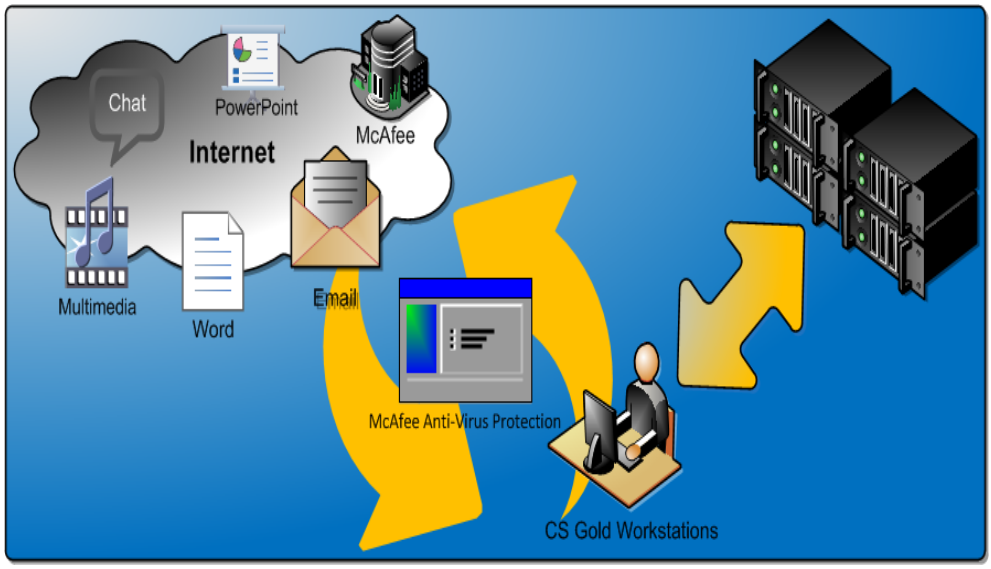
16. Workstation Security

The PantherCARD Office had 16 workstations connected to the PantherCARD system. The Office does not ensure that all applicable workstations, servers, or mobile computing devices on the network, employ mechanisms to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means.

The PantherCARD Office employs a layered security approach of McAfee antivirus, web browser settings and Microsoft Windows malicious software removal tools to detect and eradicate malicious code, also referred to as Malware. However, we observed that 15 of the 16 workstations were missing or inadequately applying one or more layers of malicious code protection. This reduces their effectiveness in mitigating the risk of malicious code transported by electronic mail, electronic mail attachments, removable media, web access, or other means.

An assessment of patch and vulnerability management, a security practice designed to proactively prevent the exploitation of Information Technology vulnerabilities that may exist within the PantherCARD Office revealed the following:

- four of the sampled workstations had outdated web browsers;
- one workstation had unnecessary services (i.e., SMTP & WWW Publishing);
- one workstation was missing Office XP Service Pack 3; and
- one workstation was missing Microsoft Office 2007 security updates.



Proactively managing vulnerabilities of information systems would reduce or mitigate the potential for exploitation and reduce the time and effort required to respond should such exploitation occur.

In responding to malicious code events, we concluded that the PantherCARD Office has adequately established and configured quarantine data control procedures. However, in order for malicious code protection mechanisms to be effective they must be maintained by automatically loading the most current releases (including new virus signature definitions) as soon as they are available. Throughout our test period virus definitions were not adequately updated for 11 of the 16 machines. Only four of the sampled workstations were updated during all of the four quarterly periods. Two workstations were never updated; the remaining workstations were updated less frequently than each quarter. Malicious code virus definitions were not properly updated by the University's Technology Service

department's ePO server, and McAfee update log files were not periodically reviewed by the PantherCARD Office.

Another effective means to mitigate the risk of malicious code infection would be to set workstations to perform real-time scans of all electronic files received from external sources (such as the web, email, and USB) as they are downloaded or opened. The periodic/scheduled scans of workstation hard drives would also be helpful in mitigating the risk of malicious code infection. All of the sampled workstations perform scans of external source files but only three of the hard drives are adequately scanned on either a daily or weekly basis.

PantherCARD virus protection mechanisms would be most effective if it were centrally managed. The PantherCARD Office is moving in the right direction in this regard as it is in the process of upgrading their workstation malicious code protection mechanisms to a centrally managed process though the University Technology Services department.

The ability to set or modify malicious code protection configurations should be limited to Information System Administrators. However, non-administrator personnel have administrator access level privileges for seven of the workstations reviewed.

An important control to mitigate the risk of unauthorized access to PantherCARD Office workstations and the critical information that they contain is to maintain the user login/lockout features of each of the workstations. However, eleven workstations did not have the account lockout features activated. This means that the workstations have a greater vulnerability to brute force access attempts. There were also inconsistent lockout parameters on the remaining workstations tested, as two workstations were configured to lockout the user only after five invalid attempts and one workstation was set to lock out the user after twenty invalid attempts. Only one workstation was set to lock out after the customary three invalid attempts.

When the lockout feature activates, it should be locked for a specified time period before allowing the user to retry; lock out the account until released by an administrator; or delay the next login prompt once an account has been locked out. For the workstations which had the lockout features activated; two workstations were locked for only fifteen minutes; one workstation was locked for thirty minutes; and one workstation was locked for an hour.

Recommendation:

The PantherCARD Office should:	
16.1	Ensure that all workstations' security features are up-to-date, properly enabled by only employees with administrative access privileges, and functioning as designed.

Management Response/Action Plan:

16.1 As part of the re-organization of the FIU One Card Office, new workstations were purchased for the entire office, and each has up-to-date security features and restricted administrative access privileges.

Implementation date: Immediately

17. Continuous Service

To mitigate the risks associated with catastrophic events, contingency planning policies and procedures must be created, reviewed, updated, approved, and tested. However, there are currently no authorized or approved Business Continuity or Disaster Recovery policies for the PantherCARD Office. Ideally, the PantherCARD Information Systems Contingency Plan should identify essential missions and business functions, associated contingency requirements, provide recovery objectives, restoration priorities and metrics, address contingency roles, responsibilities, assigned individuals with contact information; address maintaining essential missions and business functions despite an information system disruption, compromise, or failure; address eventual full information system restoration without deterioration of system measures originally planned and implemented; and be reviewed and approved by designated officials within the PantherCARD Office.

The lack of an authorized and approved contingency plan reduces the effectiveness of the PantherCARD Office's preparedness in the event of a disaster.

In a Contingency Plan, specific PantherCARD personnel would be identified as key personnel, and personnel in the University's Division of Information Technology department would be identified by name and role, as designated to receive and act upon the contingency plan.

Contingency plan testing should be defined by the PantherCARD Office which should in turn coordinate contingency planning activities with incident handling activities assigned to other FIU organizational units. Contingency plan should be revised to address changes to the PantherCARD Office, information systems, or environment of operation and problems encountered during the actual contingency plan implementation, execution or testing.

Recommendation:

The PantherCARD Office should:	
17.1	Work with the Office of Emergency Management and the Division of IT to develop, maintain and test a comprehensive, all-inclusive IT continuity framework for the PantherCARD system.

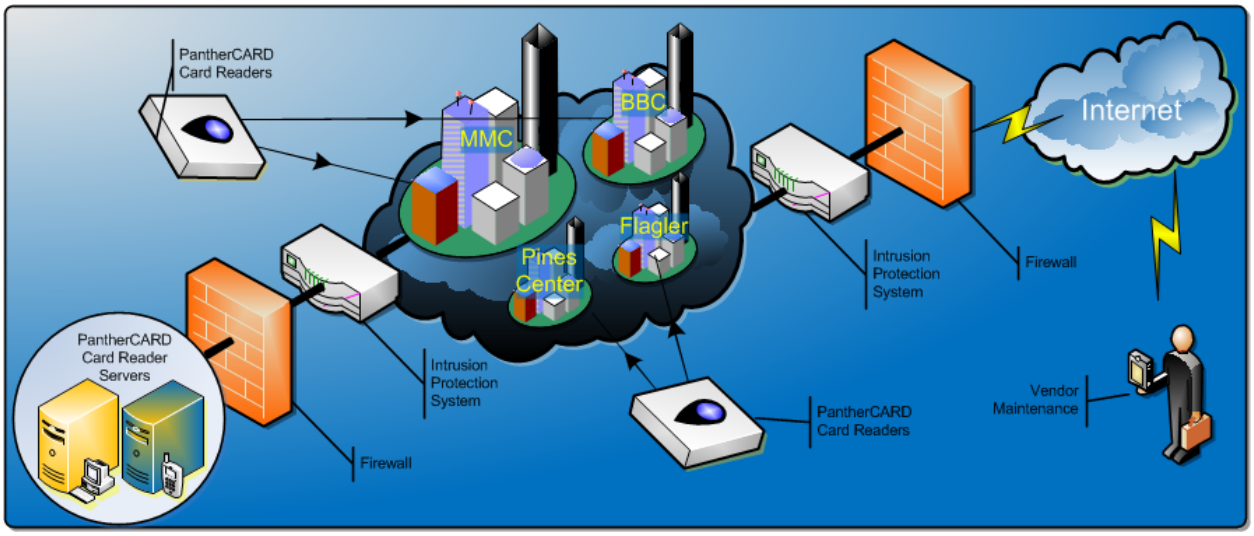
Management Response/Action Plan:

17.1 As part of the re-organization of the FIU One Card Office, the FIU One Card Office will be integrated into the emergency management system of the Office of Business Services. The Division of IT is also in the process of developing an IT Continuity Framework as part of a different audit. The Division of IT will share this framework with the FIU One Card Office once the framework has been developed.

Implementation date: April 30, 2012

18. Network Security

The University Technology Services Network Management Services Department is responsible for PantherCARD network security. The network management security adequately and effectively documented the network's external and related key internal boundaries. In all material respects network security adequately protects the PantherCARD system.



According to Network Management Services, there is no set frequency for reviewing exceptions to the PantherCARD traffic flow policy for each PantherCARD managed interface. A defined frequency for these reviews might increase the effectiveness of PantherCARD network security controls. An informal PantherCARD traffic flow policy has been established, though we did observe one "MAC address"[3] missing from the 12 traffic flow items reviewed. The Department adequately documents the review of traffic flow exceptions but the duration of PantherCARD firewall exception requests weren't documented.

Managed information system documentation adequately details intrusion protection access list settings and effectively denies network traffic by default. Based on our review of information systems security controls, we concluded that Department managed interfaces adequately allowing PantherCARD network traffic by exception.

Information systems controls were adequate and provided effective security to protect the confidentiality and integrity of the information being transmitted by the CS Gold application. Network Management Services provides a layered security approach using intrusion protection systems, firewalls, and mandatory Virtual Private Network connections to increase the effectiveness of protection the confidentiality and integrity of information being transmitted by the CS Gold application. The Department also adequately monitors events on PantherCARD information systems to effectively detect PantherCARD information systems attacks.

The Department has implemented an intrusion protection system to monitor inbound and outbound communications. The intrusion protection system signature definitions are adequately updated and implemented on a daily basis, which effectively increases the system's ability to monitor and detect communications for unusual or unauthorized activities or conditions.

[3] The Mac Address is a unique value associated with an electronic device, which allows the device to uniquely identify itself on a network. Mac Address filtering is an additional layer of network security which restricts access to only the devices registered with the router.

Network Management Services Department adequately sends real-time alerts of potential medium or high-risk indicators within 24 hours of the Intrusion Protection System's detection to appropriate incident response personnel in the Network Security and Systems Engineering ("NSSE") group to suspicious events.

Recommendations:

The Network Management Services Department should:	
18.1	Define the frequency for reviewing exceptions to PantherCARD traffic flow.
18.2	Perform a review of firewall and router rule sets every six months.
18.3	Develop a formal traffic flow policy requiring IP, MAC address, location and port number for each PantherCARD managed interface.
18.4	Ensure that PantherCARD firewall exception requests have a defined duration.

Management Response/Action Plan:

18.1 Network Engineering and Telecommunications and the FIU One Card IT staff will review on a bi-annual basis the list of open ports for the Panther Card Servers.

Implementation date: Immediately

18.2 Network Engineering and Telecommunications will provide the FIU One Card IT staff the list of open ports for the Panther Card Servers for them to review on a bi-annual basis. FIU One Card IT staff will determine and notify Network Security of any changes which need to be made.

Implementation date: Immediately

18.3 Network Engineering and Telecommunications will create a template for the FIU One Card IT Staff to follow when requesting new firewall rules. Requests will be sent from the FIU One Card IT Staff to Network Security using the template which will be developed.

Implementation date: December 31, 2011

18.4 Network Engineering and Telecommunications will work with FIU One Card IT staff to ensure that temporary firewall rules used for testing or troubleshooting are removed after they are no longer needed. FIU One Card IT staff will need to notify Network Security once they are done testing. These will also be part of the bi-annual review mentioned in response to No.18.1.

Implementation date: Immediately