Audit of the
School of Computing and Information Sciences

Report No. 13/14-15

June 26, 2014

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: June 26, 2014

To: Amir Mirmiran, Dean of the College of Engineering and Computing
Sundararaj Iyengar, Director of the School of Computing and Information Sciences

From: Allen Vann, Audit Director

Subject: **Audit of the School of Computing and Information Sciences Report No. 13/14-15**

Pursuant to our approved annual plan, we have completed an audit of the School of Computing and Information Sciences. The primary objective of our audit was to determine if the School's established controls and procedures are adequate to ensure that: (1) Information technology (IT) controls properly protect the confidentiality, integrity, and availability of sensitive and/or critical data; (2) financial/operational controls are appropriate; and (3) University policies and procedures, applicable laws, rules and regulations are adhered to.

While IT and financial controls are in place, our audit identified some areas in need of improvement, particularly IT security controls related to identity access, information systems, business continuity, network, and facilities access. The financial controls related to equipment use fee, Foundation expenses, attractive property tracking, credit card use, and travel authorization can also be improved. Additionally, opportunities for cost savings may be achieved if the School utilizes preexisting IT resources from the College of Engineering and the Division of IT. The audit resulted in 21 recommendations which management agreed to implement.

We would like to take this opportunity to express our appreciation for the cooperation and courtesies extended to us during this audit.

Attachment

C: Sukrit Agrawal, Chair, BOT Finance and Audit Committee and Committee Members
Mark B. Rosenberg, University President
Douglas Wartzok, Provost and Executive Vice President
Kenneth G. Furton, Provost and Executive Vice President-Designate
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Kristina Raattama, General Counsel
Howard R. Lipman, Senior Vice President, University Advancement
Robert Grillo, Vice President and Chief Information Officer
Javier I. Marques, Chief of Staff, Office of the President

TABLE OF CONTENTS

Page

OBJECTIVES, SCOPE AND METHODOLOGY 1

BACKGROUND 2

Personnel 3

Financial Information 4

FINDINGS AND RECOMMENDATIONS 6

1. Identity Access Management 7

a) Procedures 7

b) Unique Identification and Authentication 7

2. Information Systems Security 9

a) Endpoint Devices 9

b) Analyze Physical Surroundings 8

c) Malicious Code Protection 9

d) Media Sanitization 10

3. Network Security 13

a) Firewalls Controls 13

b) Monitoring 13

c) Remote Access 14

4. Facilities Security 17

a) Building Access 17

5. Business Continuity Plan 19

a) Planning 19

b) Testing 19

6. IT Resource Utilization 21
7. Student Fees 23
8. Foundation Expenses 24
9. Asset Management 25
10. Credit Card Controls 26
11. Travel Authorization and Expenses 27
Appendix A: User Access Lifecycle Diagram 28

OBJECTIVES, SCOPE AND METHODOLOGY

Pursuant to our approved annual plan, we have completed an audit of the School of Computing and Information Sciences (School or SCIS). The primary objective of our audit was to determine if the School's established controls and procedures are adequate to ensure that:

- Information technology (IT) controls properly protect the confidentiality, integrity, and availability of sensitive and/or critical data;

- Financial/operational controls are appropriate; and

- University policies and procedures, applicable laws, rules and regulations are adhered to.

The examination covered expenditures for the period July 1, 2012 through November 30, 2013. During the audit, we observed and tested current practices and processing techniques, Interviewed responsible personnel, and tested selected transactions. Sample sizes and transactions selected for testing were determined on a judgmental basis. Audit fieldwork was conducted from October 2013 to April 2014.

To accomplish the Information Technology (IT) control objectives, we applied a governance, risk and compliance framework, which utilizes the *Control Objectives for Information and related Technology (COBIT) 5.0 Framework and the National Institute of Standards and Technology (NIST) Special Publications 800-53A Revision 1 Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. Our audit 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.

As this was the first internal audit of SCIS, there were no prior internal audit recommendations related to the scope and objectives of this audit requiring follow-up. Similarly, there were no other external audit reports issued during the last three years with any applicable prior recommendations related to the scope and objectives of this audit.

BACKGROUND

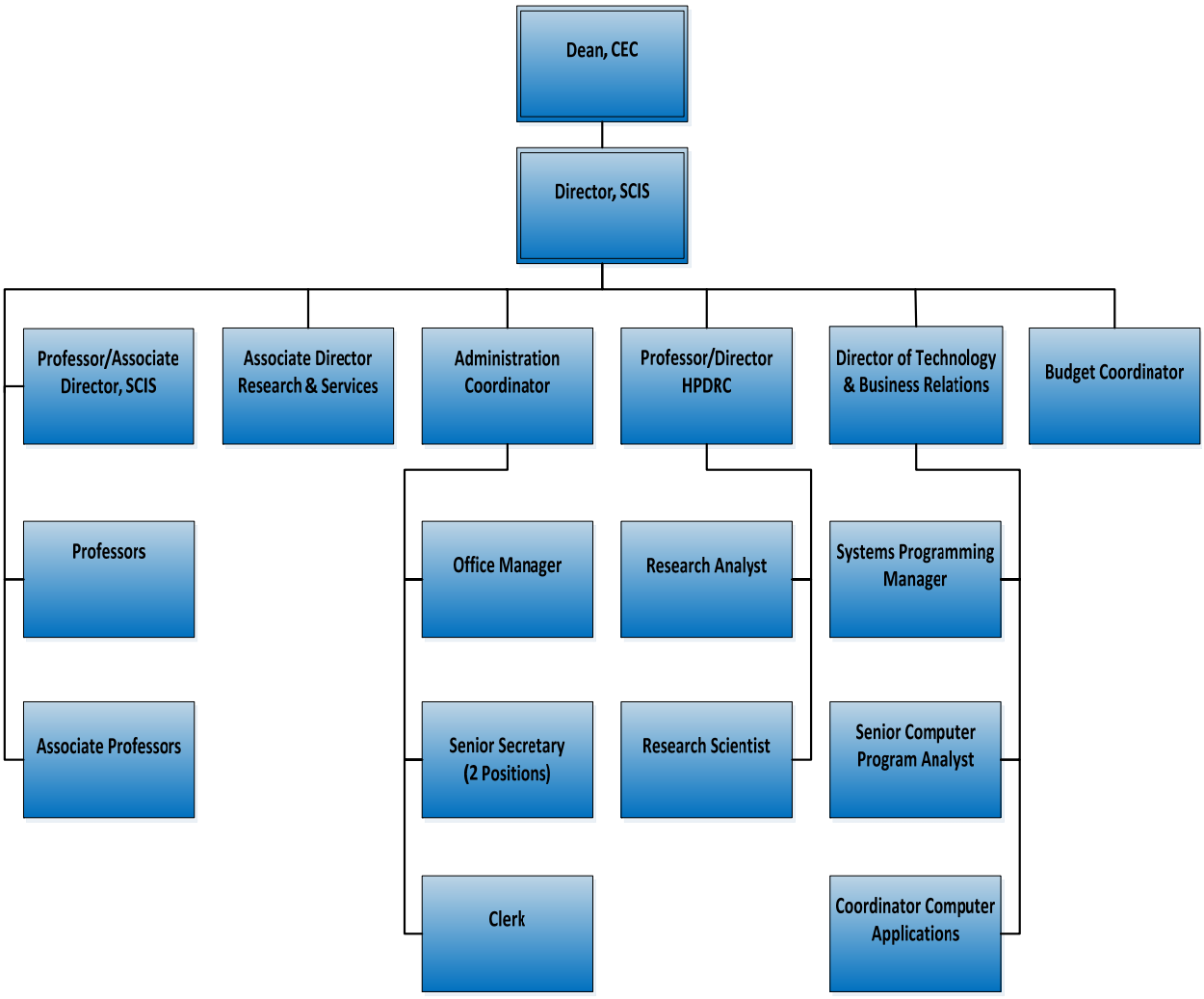
Founded in 1987, the School of Computing and Information Sciences (formerly the School of Computer Science) at Florida International University (FIU or University) offers undergraduate programs in computing and information sciences and graduate programs in computer science. In July 2005 the School of Computer Science merged with the College of Engineering. The School of Computer Science was renamed the School of Computing and Information Sciences and became part of the newly established College of Engineering and Computing (CEC).

The Computer Science (ABET/CSAB accredited) and Information Technology undergraduate programs provide students an education consisting of both the theoretical and applied knowledge necessary for a successful career as a computing professional. The research-driven Masters and Ph.D. programs provide students opportunities to conduct cutting-edge research with experienced faculty from numerous large-scale projects. According to the School, the enrollment for fall 2013 included over 1,600 undergraduate and 200 graduate students, including 79 PhD students.

The School of Computing and Information Sciences maintains a separate IT infrastructure from the University, which includes 10 Gigabit Ethernet network, email, business continuity, file services, and data center. It also provides research and instructional labs. These facilities are housed in the Engineering & Computer Science (ECS) building at the Modesto A. Maidique Campus. Appendix A contains an overview diagram of the School's User Access Lifecycle.

Personnel

As of October 2013, the School had 49 faculty and staff members. The School's organization chart is shown below.



Financial Information

During the fiscal year 2012-13, the School cost $12 million to operate. The majority of its expenditures were paid from Educational and General (E&G) funds but sponsored research and auxiliary revenues provided significant contributions totaling $4 million and $271,525, respectively. Recognizing the importance of the School's educational contributions the State of Florida has awarded it with $2.7 million in IT performance funding.

Annual expenditures by major cost categories are depicted in the following table:

Category	Amount
Salaries & Benefits:	
E&G funds	**$7,002,966**
Other than E&G funds	**2,136,713**
Subtotal – Salaries & Benefits	**$9,139,679**
Operating Expenditures:	
Furniture & Equipment	**$593,699**
Facilities & Administrative Expense	**670,977**
Scholarship, Stipend & Tuition	**481,163**
Professional Services & Advertisement	**460,075**
Supplies & Materials	**126,106**
Miscellaneous	**196,150**
Travel, Training & Entertainment	**190,307**
Telecommunications	**57,404**
Shared Service Fee (Overhead)	**34,404**
Repairs & Maintenance	**20,931**
Postage	**17,295**
Software Over $5,000	**15,750**
Legal Fees & Services	**11,760**
Sub-total - Operating Expenditures	**$2,876,021**
Total Expenditures	**$12,015,700**

(page intentionally left blank

FINDINGS AND RECOMMENDATIONS

Overall, our audit disclosed that IT security and financial controls were fair. Nevertheless, our audit identified some areas in need of improvement, particularly IT security controls related to identity access, information systems, business continuity, network, and facilities access. The financial controls related to equipment use fee, Foundation expenses, attractive property tracking, credit card use, and travel authorization can also be improved. Additionally, there is an opportunity for cost savings if the School utilizes University IT resources from the College of Engineering and the Division of IT.

Our overall evaluation of internal controls is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		**X**	
Policy & Procedures Compliance		**X**	
Effect		**X**	
Information Technology Risk		**X**	
External Risk		**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**
Information Technology Risk	**System controls are effective in mitigating identified data risks**	**System controls are moderately effective in mitigating identified data risks**	**Systems controls are ineffective in mitigating identified data risks**
External Risk	**None or low**	**Medium**	**High**

The areas of our observations during the audit are detailed below.

1. Identity Access Management

Identity Access Management controls reviewed included policies, procedures and the unique identification of user accounts. According to NIST sp800-53A Rev.1 AC-2.1, user identity and logical access, should be managed to ensure that all accounts are appropriately established, modified, and disabled in a timely manner.

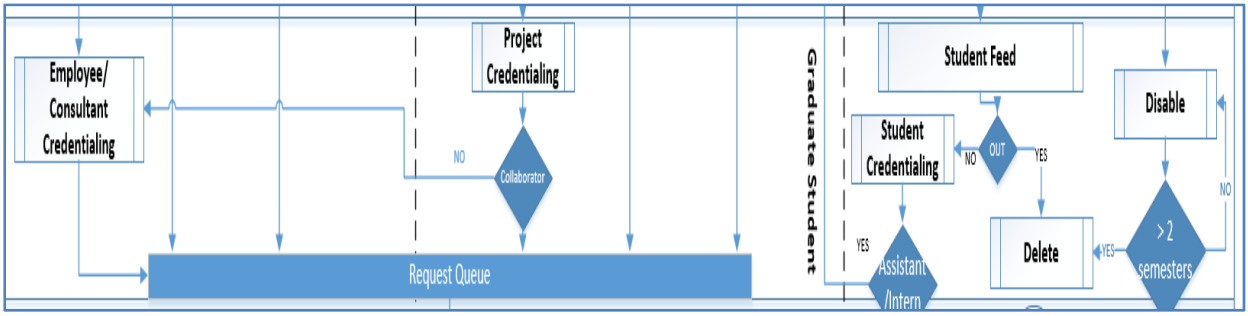


Figure 1- Identity Access Management Areas Tested

a) Procedures

The student creation process is fully automated and based on class enrollment. However, the School does not have formal Identity Access Management procedures for the faculty and staff accounts. The employee onboarding and off-boarding of user access is maintained in a web based request queue application. User access requests are sent through the application where the Information Technology department then completes the required changes. There were 1,227 and 2,680 active user accounts on the Employee/Research and Student academic networks, respectively. Testing of 23 new user and 7 transferred/terminated employee accounts revealed that:

- 14 of the 23 new users did not have corresponding user access requests.
- None of the 7 transferred/terminated users had corresponding user deactivation requests.

The lack of formal procedures and missing access request documentation increases the risk of unauthorized access.

b) Unique Identification and Authentication

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. Of the 16 selected computers tested, the windows devices had generically name user accounts; the operational server had two default user accounts and the student credentialing server had an active test account. The effectiveness of a user account's password is largely determined by its parameters particularly the maximum age of the password. The identified generically

named user accounts on the windows devices were non-expiring and the non-windows devices do not have password parameters. Passwords that are not changed regularly may increase the risk of being exploited by a malicious user. In addition, 2 non-IT personnel (Administrative Coordinator and Senior Secretary) had administrator privileges to their windows devices. This access along with generically named administrator accounts increases the risk of unauthorized access.

Recommendations:

The School of Computing and Information Sciences should:	
1.1	Establish a formal procedure to ensure that there is adequate documentation supporting the creation, modification, and deactivation of user accounts.
1.2	Review and disable generically named administrator accounts and comply with the University's password parameter settings.
1.3	Review and disable administrative privileges from the two non-IT user accounts.

Management Response/Action Plan:

1.1 Student accounts will continue to use the existing application which synchronizes account creation and deletion with PantherSoft student data. A new application will be developed to formalize the existing process of employee account change management documenting account activity in the School's trouble ticket system.

Implementation date: January 5, 2015

1.2 Dedicated Windows administrator accounts are assigned to the appropriate IT staff for accountability. Unix administrators accounts are logged via sudo. Any unnecessary administrators accounts will be removed so long as their removal does not interfere with OS/Application operation. The School shall review and update its current password management system to be consistent with the University's password management policy.

Implementation date: August 25, 2014

1.3 The Windows desktop administrator privileges will be removed from non-IT administrators employees' computers. Those users will contact our IT staff to have the necessary patches updated as needed to run University required software. Researchers will continue to have access to admin privileges so as not to impede their experimentation.

Implementation date: July 1, 2014

2. Information Systems Security

Information Systems Security includes preventive, detective and corrective measures, which are implemented and maintained (especially up-to-date security patches and virus definitions) on endpoint devices such as laptops and desktops that connect to the School's network and protects them from malware, brute force attacks and unauthorized access.

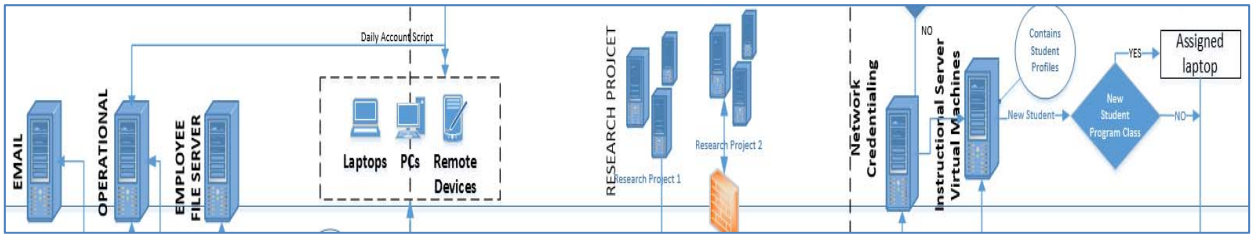


Figure 2- Information Systems Security Areas Tested

a) Endpoint Devices

According to FIU Policy 1910.005, *Responsibilities for FIU Network and/or System Administrators*, the School should maintain and make readily available a list devices which includes items such as the model number, operating system, media access control address, host name and primary user's information, physical location, and the information system's primary function. The file used to track hardware items was missing user names and location information.

Additionally, the file did not contain a data classification scheme for each of the hardware items. By classifying the devices through a risk rating scheme helps ensure that the information systems are in line with the appropriate guidelines and regulations. Missing tracking information reduces the effectiveness of the endpoint inventory list.

b) Analyze Physical Surroundings

According to FIU Policy 1930.020, Information Technology Security, the physical and logical integrity of electronic resources including networks, computers, software and data must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Three of the 16 selected endpoint devices had exposed passwords, in the form of sticky notes and letter paper, around their device physical surroundings. The exposed passwords increase the risk of unauthorized access to the School's electronic resources.

c) Malicious Code Protection

According to FIU Policy 1930.020c, *System and Application Management*, all University-owned computing hosts that are subject to virus infection must have antivirus software running. In addition, all computers owned by the University, regardless of which operating system they use, must have current and appropriate operating system

and application software patches applied. Our test of 16 endpoint devices revealed that:

- 9 Windows devices had their McAfee On-Access Scanner and Windows Malicious Software Removal Tool up to date.
- 6 of the 7 non-Windows devices did not have antivirus protection.
- 3 non-Windows servers did not have their operating system patches installed in a timely manner.

Without an antivirus solution, operating system patches that are not applied in a timely manner increase the risk of data being compromised.

According to the FIU Procedure 1930.020c, *System and Application Management*, it is the responsibility of the School's information system administrator to enforce system and antivirus updates. The School maintains an open source email server, which is separate from the University's system. An open source antivirus solution was implemented on the email server to check emails for viruses and its definition files were automatically updated. Per documentation provided by the School showed 230 devices' installed legacy operating systems which are unsupported by the vendor and no longer receive security updates and patches.

Antivirus solutions are reduced in their effectiveness to protect against malicious code if security mechanisms are not implemented and kept current with the latest security patches. Devices that are running operating systems without vendor support increase the risk of data compromise.

d) Media Sanitization

If proper steps are not taken to destroy information contained on hard drives, the information from the disposed media may be retrieved by an unauthorized individual. As required by FIU Draft Policy Media Sanitization Procedures, the School sent an email to the University's Information Technology Security Office (ITSO) a list of each individual IT equipment that is ready for surplus. The email adequately included the description, serial number, FIU Tag number and is followed up by the ITSO with an MSCID number. The surplus of the School's IT equipment is adequately performed.

Recommendations:

The School of Computing and Information Sciences should:	
2.1	Review and complete missing inventory list information.
2.2	Perform a data classification to ensure that the high risk and/or sensitive information systems are maintained in accordance with appropriate guidelines and regulations.
2.3	Review and remove the exposed passwords from their physical surroundings.
2.4	Implement an antivirus solution on its non-Windows devices and implement all operating system patches in a timely manner.
2.5	Review endpoint devices to ensure that operating system patches are supported by the vendor.

Management Response/Action Plan:

2.1 We will increase the frequency of updating inventory log files, to each semester to insure change management consistency.

Implementation date: August 25, 2014

2.2 The School will conduct a formal data classification study and evaluate and enhance current best practices to secure high risk and/or sensitive system per university, state and federal policies.

Implementation date: August 25, 2014

2.3 The School will continue to conduct sweeps of all equipment to insure all exposed passwords are removed. Staff and students will be periodically reminded of security best practices as provided by the IT Security Office.

Implementation date: July 1, 2014

2.4 In addition to TripWire, the School will run ClamAV (unix/linux) software on non-window systems. Other products will be evaluated to determine best fit. The School will continue to apply security related and mandatory OS patches on all systems in accordance with vendors' best practices and address those not in compliance. In the case of research systems which have legacy experiments where the above will impact operations other precautions will be implemented.

Implementation date: August 25, 2014

2.5 The School will continue to conduct reviews of endpoint devices such as desktop systems and printers to ensure that the manufacturer is providing OS patches, as needed.

Implementation date: August 25, 2014

3. Network Security

Network Security includes defining and protecting internal and external boundaries; limiting access points to the boundaries through the use of firewall to allow for more comprehensive monitoring of inbound and outbound traffic; document exceptions to the implemented firewall rules; and protecting the information during transport outside of controlled areas.

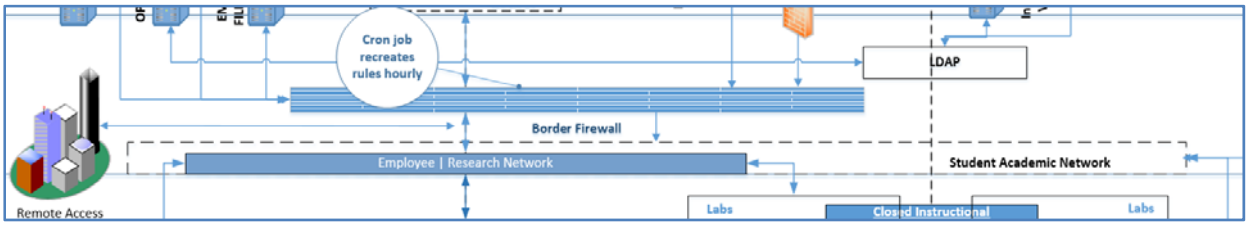


Figure 3- Network Security Areas Tested

a) Firewall Controls

Firewalls and routers are key components of the architecture that controls entry into and from the School's network. Network diagrams describe how networks are configured and without a current diagram, devices could be overlooked and be left out of implemented network security controls. The School has a current network diagram which defines the external network through two outer border routers: a segmented part of the network to define the DMZ[1] border; and a VRRP[2] router that defines the internal network boundaries.

The main firewall's rule sets adequately document the purpose of the implemented rules. By clearly defining and documenting the rules helps to ensure that all rules and ports are disabled or removed as needed. Firewall rules are created on an hourly basis through an automated script, which checks the available hosts' information and then builds the inbound and outbound rule blocks of the main firewall.

There was one identified host device that was incorrectly listed in the host files. It was listed as part of the School's network but was actually located in the University's data center. Although the device did not have an associated firewall rule, it does raise the concern of the potential negative effect on the automated script's ability to open ports for devices not actually available.

b) Monitoring

Though firewalls block unwanted access and manage network traffic into and out of the network, it is necessary to monitoring these devices. The School monitors its network traffic though the examination of Bits per Second diagrams to pinpoint Distributed

[1] The DMZ is a firewall configuration used to secure local area networks.
[2] Virtual Router Redundancy Protocol provides automatic IP assignment to increase the reliability of routing paths.

Denial of Service (DDoS) attacks and not through the University's Intrusion Protection System (IPS). Additional methods such as internal and external vulnerability scans that run against selected devices and servers help to identify potential security gaps that could be located by malicious software. The School's IT department runs nightly port scans from within the internal network that is behind the firewalls. According to the Assistant Director of the Information Technology Security Office, their office has never performed a vulnerability scan on the School's outbound facing network controls. The lack of the additional security layers provided by connecting to the IPS and external vulnerability scanning reduces the likelihood that vulnerabilities are identified and corrective measure taken in a timely manner.

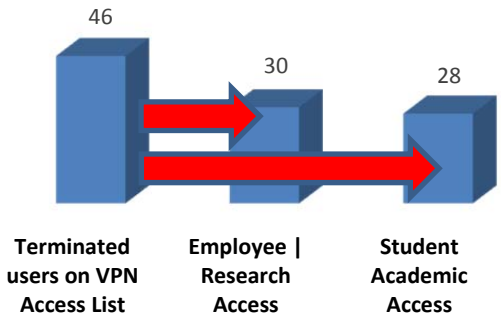
c) Remote Access

Per COBIT 5.0 DSS05.02.07, trusted mechanisms should be implemented to support the secure transmission and receipt of information over all methods of connectivity. Outside connection to the School's network is available through the use of a Virtual Private Network (VPN).

Of the 149 active VPN users:

- 5 VPN users not affiliated with the School did not have a corresponding request ticket.
- 46 of 53 terminated users were still listed on the VPN user list.
- 30 of the 46 terminated user accounts listed in the VPN user list had access to the employee/research network. On average, the users still had VPN access to the network for 835 days after their termination.
- 28 of the terminated user accounts listed in the VPN user list had access to the student academic network. On average, users still had VPN access to the network for 789 days after their termination.

Terminated Users with VPN Access



The lack of timely removal of terminated users from the VPN list and user accounts without a corresponding request ticket increase the risk of unauthorized access.

Recommendations:

The School of Computing and Information Sciences should:	
3.1	Review and update the main hosts file to ensure the accuracy of the listed information.
3.2	Establish periodic external vulnerability testing with the Information Technology Security Office and work with the Network Security Systems Engineering department to connect devices, where appropriate, to the University's IPS.
3.3	Review and remove unauthorized users from the VPN list; periodically review the VPN list to ensure that unauthorized users are removed in a timely manner.

Management Response/Action Plan:

3.1 As per recommendation 2.1 the main host files will be regularly updated and reviewed.

Implementation date: August 25, 2014

3.2 The School will work with the Information Technology Security Office to conduct external vulnerability testing via services they provide. Per recommendation 2.2 the School will continue to evaluate systems at high risk and implement best practices to secure such systems.

Implementation date: January 5, 2015

3.3 The VPN list will be reviewed on a semesterly basis to insure that unauthorized users are removed.

Implementation date: August 25, 2014

(page intentionally left blank)

4. Facilities Security

The purpose of Facilities Security is to prevent unauthorized persons from gaining access to sensitive areas and potentially steal, disable, or disrupt the School's operations.

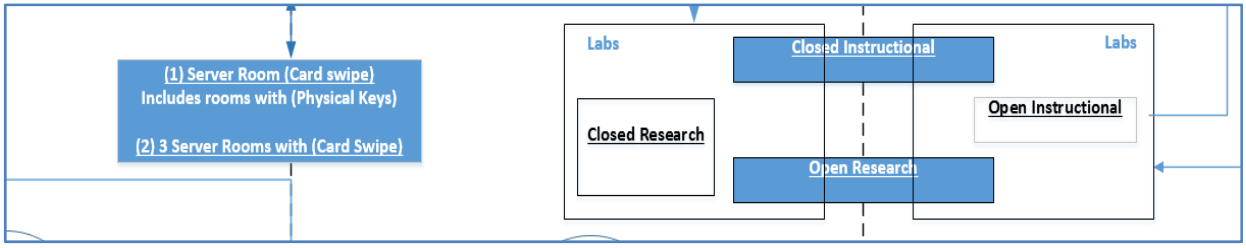


Figure 4- Facilities Security Areas Tested

The Systems Programming Manager is accountable to the appropriateness of the access to the sensitive areas while the University's Key Control Department is responsible for the building's access mechanisms. There are 3 server rooms, 13 closed research labs and 1 closed instructional lab that require a University ID card to access these areas. Additional security controls include the use of video monitoring of all entryways to classrooms, labs and server rooms and the review of user access logs every 3 months on an informal basis.

a) Building Access

The School uses a request queue application to document physical access to the restricted areas, which ensures that only authorized personnel with a legitimate business need are granted access. Building access requests are sent through the application where the systems programming manager would grant or revoke access. Testing of 16 new hires, 6 transfers, and 47 terminated employees found that:

- No transferred or terminated users had access to the any of the 3 server rooms.
- 8 new users did not have a corresponding ticket request for building access.
- 1 transferred and 6 terminated users had access to research labs for 212 days on average after it was no longer required.

The lack of documented access requests and untimely removal of terminated users increase the risk of unauthorized building access.

Recommendation:

The School of Computing and Information Sciences should:	
4.1	Work with the University's Key Control Department to ensure that building access is documented, appropriate, and removed in a timely manner.

Management Response/Action Plan:

4.1 As part of our response to Recommendation 1.1, requests for access to rooms will be formalized via the School's trouble ticket system.

Implementation date: August 25, 2014

5. Business Continuity Plan

The purpose of Business Continuity is to establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operations of critical business processes at a level acceptable to the School.

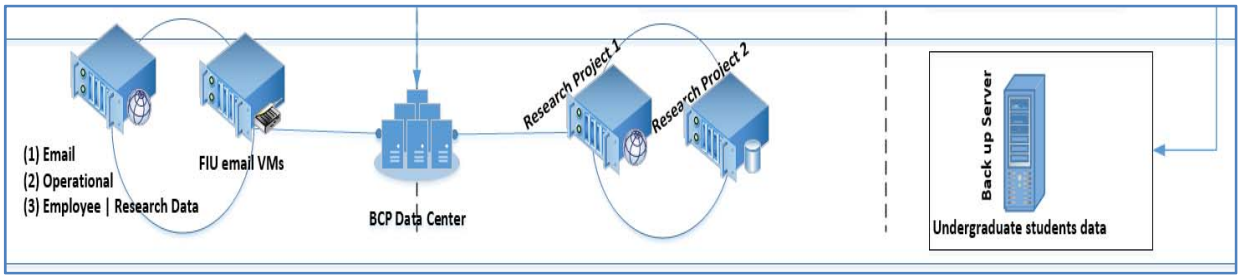


Figure 5- Business Continuity Areas Tested

a) Planning

The continuity plan was created in March 2014 and documented the plan's purpose, coordination among entities, and roles and responsibilities. However, there was not a defined time period to review and update the plan. Without regular a scheduled review period, the continuity plan may become outdated and reduce its effectiveness.

The plan identifies 5 essential IT services, which include the (1) File servers, (2) email server, (3) Moodle, (4) Web server, and (5) research servers. The systems program manager and senior computer program analyst are responsible for maintaining these servers and related systems. In addition, the plan is adequately distributed to key personnel and the Administrative Coordinator is responsible for maintaining the distribution list.

The plan also lists alternate methods that can be used by faculty and staff in the event of a disaster to access webmail, network files and the School's website. However, undergraduate data is backed up locally and not to the off-site Business Continuity Data Center. By not providing off-site back up, there is an increased risk that undergraduate student curriculum data would not be available in the event of a disaster.

b) Testing

According to COBIT DSS04.04, it is a good practice to test the continuity plan on a regular basis against predetermined outcomes to help verify that the plan will work as anticipated. During our audit it was not evident that testing had taken place, although the Director of Technology and Business stated that the email system is tested annually and the file services and web server backups are reviewed on a weekly basis on an informal basis. Without formal testing, key areas could be missed that would result in reducing the plan's overall effectiveness.

Recommendations:

The School of Computing and Information Sciences should:	
5.1	Add a review time period to the continuity plan to keep the plan current.
5.2	Identify and ensure that any mission critical data is backed up at an offsite location to ensure its availability in the event of a disaster.
5.3	Formalize the continuity plan's testing, test results, any corrective actions taken to ensure the continuance of all mission critical services in the event of a disaster.

Management Response/Action Plan:

5.1 Finalize the current Continuity plan. Thereafter, the School's Business Continuity plan shall be reviewed and updated in March of each year.

Implementation date: August 25, 2014

5.2 In addition to existing backups that are already being performed for mission critical data, the School will evaluate and add additional storage as needed to continue mission critical operations in the event of disaster.

Implementation date: January 5, 2015

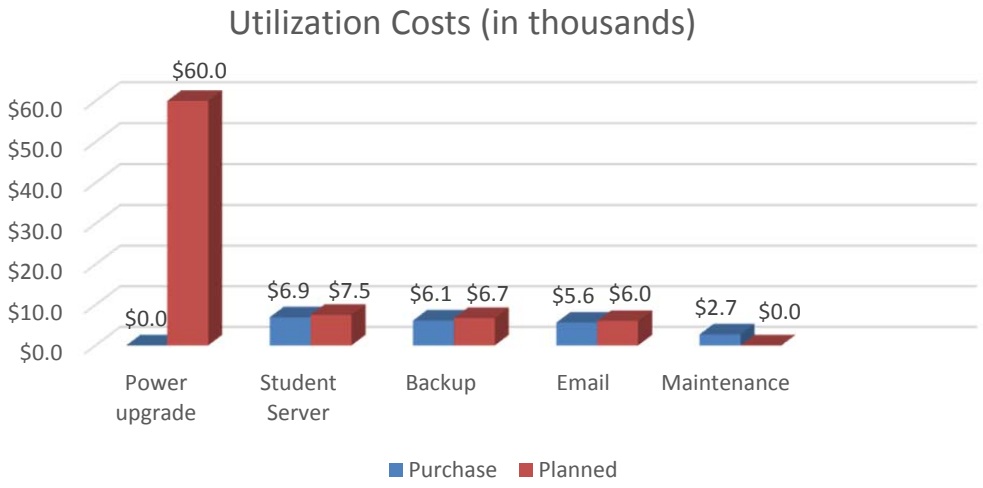
5.3 Per 5.1, a formal continuity testing plan of the School's IT services will be documented. Test results and corrective actions will be logged.

Implementation date: January 5, 2015

6. IT Resource Utilization

One of the reasons for merging the School of Computer Science with the College of Engineering in 2005 was to combine resources to efficiently provide students with a better, more comprehensive approach to the new frontiers in computing hardware and software/telecommunications and advanced applications. There are still distinctly different IT operating environments between the School, the College and University Technology Services where there is room for consolidation. According to the University's Facilities department, the ECS building, where the School's servers are located, is close to design capacity for electrical power supply. By not utilizing the other University data center resources, approximately $60,000 will need to be spent on upgrading the School's server room to support additional server racks. Some of the other resultant incremental expenditures, not including personnel costs, are identified below:

- $6,954 with a replacement cost of $7,500 for maintaining the undergraduate students' data server.
- $6,197 for additional backup server with an estimated replacement cost of $6,700 located at the Northwest Regional Data Center (NWRDC) in Tallahassee.
- $5,673 with an estimated replacement cost of $6,000 to maintain its own email server.
- $2,700 annual maintenance cost for the email, operational, and research data servers at NWRDC.



By using existing University IT resources, that already exist at the College of Engineering and the Division of IT, the School could repurpose amounts budgeted for these and similar expenditures its other educational priorities.

Recommendation:

The School of Computing and Information Sciences should:	
6.1	Review the cost and benefits of maintaining duplicative services with a view towards using centralized IT resources whenever possible (e.g. e-mail, personnel, data center, servers, and network).

Management Response/Action Plan:

6.1 The School will continue to evaluate opportunities to utilize University Technology Services resources so long as they do not impede the School's research and instructional objectives and effectiveness. An analysis will be conducted by the School in Fall for such services for review by faculty and the School Director.

Implementation date: January 5, 2015

7. Student Fees

The School of Computing and Information Sciences may assess optional fees provided that the proceeds are used for the instruction of the course and equipment or material/supply is used directly by the students. Accordingly, an Equipment Use fee of $26 for undergraduate and $16 for graduate students were collected. Students also paid a $2 Material & Supply fee per applicable course. The School's total expenditures for Equipment Use fees and Material & Supply fees from July 1, 2012 to November 30, 2013 were $194,476 and $12,462, respectively.

Our review of $169,586 Equipment Use fee expenditures disclosed that equipment totaling $10,095 was not used directly by students. For example, ten computers totaling $9,780 were purchased and placed in the classrooms for instructors' use. One tablet costing $315 was purchased for testing to replace the 40 netbooks currently used for assisting the School's administration of course evaluations. These 40 netbooks costing $11,180 were also acquired using Equipment Use fees collected from the students in the past.

Not using equipment use fee collected from students for the intended purpose will increase the School's program risk.

Our review of the material & supply fee expenditures revealed that the items purchased were properly used for student labs and directly benefited students.

Recommendation:

The School of Computing and Information Sciences should:	
7.1	Ensure that all expenditures for Equipment Use are limited to items used directly by the students.

Management Response/Action Plan:

7.1 The School has an existing practice and procedure to limit expenditures for Equipment Use and Supply and Material funds. To eliminate the minor ambiguity cited the School shall clarify the practice to authorize "only equipment used solely by students for instructional activities."

Implementation date: July 1, 2014

8. Foundation Expenses

As part of our audit, we examined Foundation related expenses, totaling $11,795. For the most part, the expenditures reviewed were made in accordance with University and Foundation requirements. However, in several related instances Foundation procedures, were not followed.

Our review of an SCIS faculty member's reimbursement from the FIU Foundation for 7 business meals totaling $1,475 disclosed that for 5 meals the employee's spouse was a participant. When a faculty or staff member's spouse participates in events, the department's corresponding Vice President or designee must approve the expense, which should include an explanation of how their participation benefits the university. The employee, however, did not disclose this relationship, which if disclosed would have required the dean's approval. We discussed the matter with the faculty member and he explained that his spouse is a participant/contributor to the FIU business related subject matter of the meetings and was unaware that it was still necessary to obtain the required additional approval for the expense report.

Recommendation:

The School of Computing and Information Sciences should:	
8.1	Remind employees to disclose the participation of their spouse on business meal expense reports along with an explanation of the benefit to the University of their participation.

Management Response/Action Plan:

8.1 The School's Director shall remind employees once a year of these important university policies regarding business expenses.

Implementation date: August 25, 2014

9. Asset Management

Per the University's asset management system, the School had 150 capital assets with associated cost totaling $2,617,150. The School's capital asset inventory as recorded in the system is up to date. We also confirmed with the Assistant Controller for Asset Management that they did not observe any missing capital assets while taking their annual physical inventory in 2013.

In addition to capital assets, the University's Property Control Manual defines attractive property as "…University property costing less than the threshold amount of $5,000, but which are particularly vulnerable to theft and misuse." The Property Control Manual recognizes that "Attractive" property items may vary from department to department, the manual offers such things as laptops, iPads, or video recorders as examples. In evaluating "attractiveness" in the context of their own environment the factors they are asked to consider include the security of the property location, the size and portability of the item, and its potential resale value if stolen. Attractive items are to be marked as University property and catalogued by the user department. Special property tags are available upon request from Property Control.

During the audit, we noted that the School maintained a database to record SCIS attractive property. However, a review of the database showed that equipment purchased using one of the School's three University credit cards was not being reported to the database manager and hence not being tracked. For example, a 3D printer costing $1,000 and a network marine AIS receiver costing $669, both of which were reportedly located off campus, were not included in the database. Reviewing all purchases would enable the school to determine, which items it needs and/or wants to include in its database. Therefore, strengthening current procedures in this regard would increase required accountability over attractive or sensitive property.

Recommendation:

The School of Computing and Information Sciences should:	
9.1	Review all purchases to ensure that attractive property is properly accounted for.

Management Response/Action Plan:

9.1 Faculty will be reminded annually of the School's longstanding policy and procedure requiring that all purchases of technology shall be registered with the School's Technology Group so that equipment, including attractive property, can be maintained in the master inventory list. The School's financial coordinator will work with the Technology Group to periodically analyze procard purchases and insure that these purchases are subject to the policy and procedure noted above.

Implementation date: August 25, 2014

10. Credit Card Controls

Except as noted below, our audit disclosed that the credit card transactions made by the School were properly approved, allowable, and in accordance with University policies and procedures. Our test of 42 credit card transactions totaling $10,559 disclosed the following exceptions:

- Two transactions totaling $710 were miscoded to incorrect ledger accounts; $60 DSL charge was coded as postage and a $650 conference registration fee was coded as local telephone.
- One transaction costing $60 was automatically charged by the vendor and approved by the approver based on a copy of a credit card payment receipt without description of goods or services. According to the University Credit Card Administrator, automatic payment using a University credit card is not allowed.
- Two transactions totaling $44 were made for cleaning supplies for the School's employee lounge. These are unallowable expenditures according to University Credit Card Solutions Policies.

Proper use of University credit cards will prevent or reduce unauthorized or unnecessary SCIS expenses.

Recommendation:

The School of Computing and Information Sciences should:	
10.1	Ensure that all credit card purchased are properly classified and comply with University credit card policies and procedures.

Management Response/Action Plan:

10.1 The School's credit card managers will continue to review statements for proper classification. ProCard holders will be reminded annually to review current ProCard policies and attend ProCard training as required.

Implementation date: August 25, 2014

11. Travel Authorization and Expenses

According to Florida Statute section 112.061(3)(a): "All travel must be authorized and approved by the head of the agency, or his or her designated representative, from whose funds the traveler is paid. . . ." Also, University Travel Expense Policy No. 1110.060 requires that: ". . . Travelers are not to make commitments to travel or to incur travel expenses without first obtaining the appropriate approval."

Testing of the 43 Travel Authorizations (TA) totaling $95,569 revealed that 24 TA were completed after the fact. The days to complete the 24 TA ranged from 1 to 111 business days after the traveler's departure date. The reimbursable expenditures associated to the 24 TA totaled $43,868. In order to ensure the propriety of travel and related expenditures, the School must align its practices with State and University requirements.

Recommendation:

The School of Computing and Information Sciences should:	
11.1	Ensure that employees obtain Travel Authorization prior to incurring travel expenses or traveling.

Management Response/Action Plan:

11.1 The School's Administrative Coordinator shall require that employees obtain Travel Authorization prior to incurring travel expenses. Faculty has been informed and will be reminded annually that: "ALL travel on university business MUST be pre-approved via an approved TA –or- no reimbursement will be issued." Faculty has also been informed to advise their students accordingly.

Implementation date: July 1, 2014

Appendix A: User Access Lifecycle Diagram