FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of the Herbert Wertheim College of Medicine Information Systems Security Controls

Report No. 12/13-04

October 1, 2012

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: October 1, 2012

To: John Rock, Dean, Herbert Wertheim College of Medicine and Senior Vice President for Medical Affairs

From: Allen Vann, Audit Director

Subject: **Audit of the Herbert Wertheim College of Medicine Information Systems Security Controls, Report No. 12/13-04**

We have completed an Audit of the Herbert Wertheim College of Medicine (HWCOM) Information Systems Security Controls. The College's IT department has a budget of over $1 million with an IT staff of nine employees and an information systems infrastructure that now includes Microsoft® Windows© operating systems desktops and servers, and virtualized hosted online applications along with their backend SQL Server databases.

The objectives of our audit were to determine whether established internal security controls and procedures over protected data are: (a) adequate and effective; (b) being adhered to; and (c) in accordance with University policies, procedures, applicable laws, rules and regulations.

As would be expected with a newly established college, and its respective IT Department, most of the processes we tested during the audit period were either informal and/or not documented. Overall, information technology controls need improvement to reduce the risk of data breaches and increase the confidentially, integrity, and availability of its sensitive data. A total of 25 of 42 control activities tested need improvement to ensure that they achieve their objectives. It is evident from management's response to our recommendations that they are moving forward rapidly on improving IT controls.

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, Interim Executive Vice President & Provost
Liane Martinez, Executive Association Dean, Finance Administration

TABLE OF CONTENTS

BACKGROUND

Florida International University's Herbert Wertheim College of Medicine provides medical education giving due consideration to South Florida's diverse demographics. The State Board of Governors authorized the College of Medicine (HWCOM or College) in March 2006. In 2007, HWCOM hired an Information Technology Director.

At the time of HWCOM's 2009 fall semester inaugural class, their IT Department consisted of a staff of five, including the IT Director, Systems Administrator, Computer Support Specialists, and an Applications Support Specialist. With an approved 2011-12 IT budget of $1,282,888, the IT staff has grown to nine employees with the addition of web development, Applications support specialist, and Field Support Technicians.

The information systems infrastructure now includes Microsoft® Windows© operating systems desktops and servers; and virtualized hosted online applications along with their backend SQL Server databases. Applications have been developed and implemented as the College continues to expand. These applications include:

- The ability for inquiring students to apply online through secure communication mechanisms, where staff members can review student credentials.

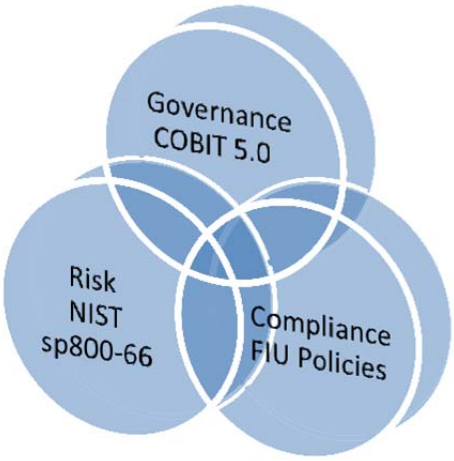
- Student psychological services provided through the Counseling and Wellness Department.

- Recording health-related data on-line while visiting patients at various South Florida locations.

The importance of data backup has increased as the information systems infrastructure has been completed. In the last quarter of 2011, the College has begun to implement its Business Continuity infrastructure to protect the confidentiality, integrity and availability of its sensitive data. The infrastructure includes Storage Area Networks (SAN) and Redundant Array of Independent Drives (RAID) which are connected to an offsite location.

OBJECTIVES, SCOPE, AND METHODOLOGIES

The objectives of our audit of the HWCOM's Information Systems Security Controls are to determine whether established security internal controls and procedures over protected data are: (a) adequate and effective; (b) being adhered to; and (c) in accordance with University policies, procedures, applicable laws, rules and regulations.



Our audit included the Information Systems security controls in place for the period from June 1, 2011 through December 31, 2011 and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*, and included tests of the information systems security controls and such other auditing procedures as we considered necessary under the circumstances.

Audit fieldwork was conducted from February 2012 to May 2012. The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes[1]. To achieve our IS audit objectives, we applied the following Methodologies and Guidelines:

- The Control Objectives for Information and related Technology (COBIT) 5.0 Framework;
- The National Institute of Standards and Technology (NIST) Special Publications 800-66 Revision 1 Introductory guide to implementing the HIPAA Security Rule; and
- Florida International University Official Policies.

During the audit, we reviewed University policies and procedures, and applicable Florida Statutes, observed current practices and processing techniques, interviewed responsible personnel, and tested the selected controls. Sample sizes and controls selected for testing were determined on a judgmental basis.

The report focuses on the COBIT 5.0 Framework and maps HWCOM related key activities to NIST HIPAA Security Rule key controls guidelines, where applicable. The Governance, Risk, and Compliance methodology provides the report with a multi-layered approach to good security practices for all protected sensitive data.

[1] Institute of Internal Auditors 2011 International Professional Practice Framework Standard 2120

Internal Control Process Capability Model

We measured the effectiveness of existing internal control processes by using the COBIT 5.0 model for process achievement assessment levels. These capability levels were then combined and calculated for each report section's Process Capability Model Rating.[2] There are six levels of capability that a process can achieve, including an "incomplete process" designation if the practices in it do not achieve the intended purposes. Lower capability ratings indicate higher inherent risk.

Previous process must be fully achieved before attaining higher capability rating

Process capability analytics, provided by COBIT 5.0, are calculated by the six levels that a process can achieve:

0 = **Incomplete process** is a process that is either not implemented or does not achieve its intended purpose. At this level, there is not enough evidence that the process achieves its intended purpose.

1 = **Performed process** is a process which achieves its intended purpose.

2 = **Managed process** is a Performed Process which is implemented in a managed fashion (planned, monitored and adjusted) to achieve its intended purpose.

3 = **Established process** is a Managed Process which is defined (documented) to achieve its intended purpose.

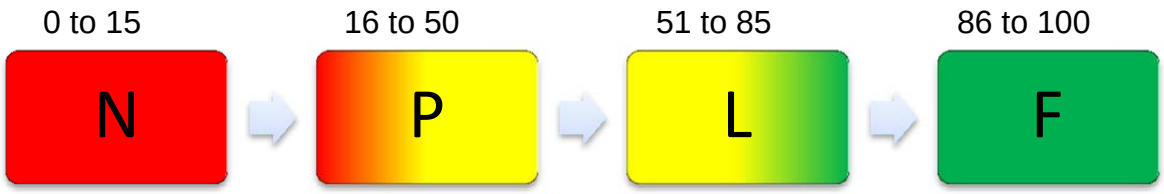
4 = **Predictable process** is an Established Process which operates within defined limits to achieve its intended purpose.

5 = **Optimized process** is a Predictable Process which is continuously improved to meet its intended purpose.

[2] Our report is divided into three sections: 1) Administrative; 2) Physical; and 3) Technical controls.

Achievement Rating Levels

By using achievement ratings measures we were able to identify the level of established internal controls effectiveness as compared to control activities outlined in COBIT 5.0, NIST special publications, and Florida International University policies. Higher rated processes are determined to be more reliable.



COBIT 5.0's achievement rating scale consists of the following:

N = Not achieved (0 to 15%)

- Internal controls which successfully passed 15% or less of our sample testing indicate that the controls are either deficient or non-existent. These controls need improvement to ensure their reliability.

P = Partially achieved (16 to 50%)

- Internal controls which successfully passed more than 15% and up to 50% of our sample testing indicate that there is some evidence that processes are in place. At this level though some aspects may be unpredictable and are not considered reliable.

L = Largely achieved (51 to 85%)

- Internal controls which successfully passed more than 50% and up to 85% of our sample testing indicate that there is evidence of a systematic approach and significant achievement of the assessed process. At this level, some weaknesses may exist within the control and improvements can be made to further improve reliability.

F = Fully achieved (86 to 100%)

- Internal controls which successfully passed over 85% of our sample testing indicate that there is evidence of a complete and systematic approach and full achievement of the assessed process. No significant weaknesses were found and these controls are considered reliable.

FINDINGS AND RECOMMENDATIONS

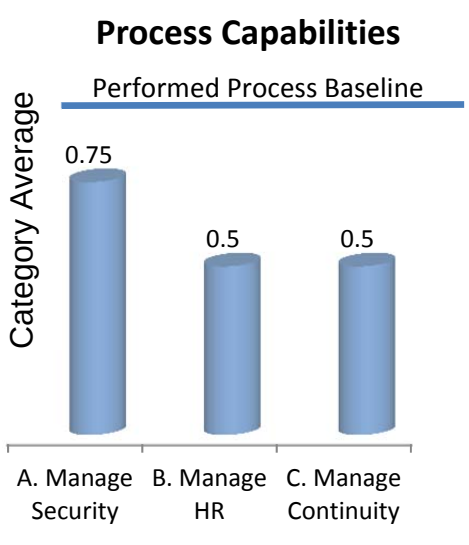
As would be expected with a newly established college, most of the processes we tested during the audit period were either informal and/or not documented. It is evident that the College is moving forward and the formality and documentation of its systems are improving.

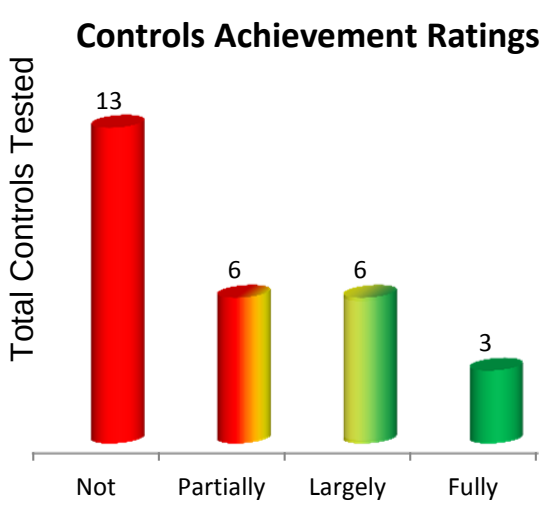
Overall, information technology controls need improvement to reduce the risk of data breaches and increase the confidentially, integrity, and availability of its sensitive data. A total of 25 of 42 control activities tested need improvement to ensure that they achieve their objectives.

Our report is divided into three information systems control sections: 1) Administrative; 2) Physical; and 3) Technical. Details of our findings and recommendations follow:

1. Administrative Controls

Administrative Controls are the administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to safeguard protected data, to manage the conduct of the personnel in relation to the protection of that information, and to continue operations of critical business processes.





We tested three areas within Administrative Controls and found that 19 of the 28 control activities selected need improvement in order to ensure that they meet their objectives. Improvements should be made to formally identify which information systems contain sensitive data; limiting access to those systems; and in implementing a continuous security awareness program. This will give HWCOM's IT Department a clearer

indication of potential risks and where to implement security controls. Workstations security should be improved by periodic reviews to ensure automated antivirus controls are functioning properly. Other areas in need of improvement are in following up on terminated users to ensure their system access is disabled in a timely manner. Continuous Security Awareness Training should be implemented to reinforce employees' understanding of their role in protecting the confidentiality of sensitive data.

HWCOM has implemented business continuity information systems infrastructure. Stronger Contingency Planning documentation will help ensure that the College of Medicine is adequately prepared in the event of a disaster. A Business Impact Analysis will ensure the availability of sensitive data by defining items, such as:

- Hardware and software restore times
- Backup methods
- Critical business operations
- Alternate operational methods

Once all of this information is properly prepared, the Business Continuity Plan should be adequately tested to ensure the plan's effectiveness in providing the continuation of critical operations.

Performed informally by HWCOM, internal evaluations need greater improvement when performed to formally identify security gaps in the above Administrative controls and ensure existing controls are operating effectively. Greater emphasis should be placed in formally identifying high risk areas and implementing mitigating controls.

A. Manage Security

According to COBIT APO13.01, APO13.02, and DSS05.01, an information security management system (ISMS) should be established that provides a continuous approach to the security management of its information assets and includes internal ISMS audits at planned intervals. The ISMS should include preventive measures to protect the information systems from malware that is implemented through viruses.

The College of Medicine's IT Department maintains a spreadsheet of the College's 50 physical/virtual servers. The spreadsheet identifies the server name, service tag, hardware model, operating system, server role, applications running, public and private IPs, VLAN, ID, and the location. However, the spreadsheet does not formally identify which of the servers store or transmit protected sensitive data; which systems are critical to the operations; or who are the servers' system owners. Tracking this type of information would formally identify which systems should be included in risk assessments.

Evaluating the potential risks and vulnerabilities to the confidentiality, integrity and availability of sensitive data is a critical control activity. In December 2011, the IT Director performed a risk assessment which included an informal walk-through of all

coverage areas, policy and procedure review, assignment of levels of risk, and availability to sensitive data. The results from the review were not formally documented.

There are frameworks available, such as COBIT 5.0 MEA02, to guide in self-assessments and independent assurance reviews. They should be continuously performed to enable management to identify control deficiencies and to initiate improvement actions. The College of Medicine utilizes a mix of internal staff, IT security, and external consultant assistance when monitoring their internal controls. Penetration tests, conducted by the Information Technology Security Office (ITSO), include over 110 information systems located on the College of Medicine's network.

Evaluation participants and data collection methods should be determined prior to conducting evaluations including interviews, surveys, system logs, and the results from penetration tests. One evaluation was performed by the College of Medicine's internal staff. An external consultant provided a brief one-day risk analysis session to the IT Director but did not participate in the evaluation. The evaluation performed by internal staff was informally conducted and did not use any of the data collection methods listed above.

Evaluation results should include test findings, remediation options and recommendations, and remediation decisions. Results should also document acceptance of any gaps identified between risks and mitigating security controls. Penetration test reports performed by the ITSO include overall risk trend statistics, total vulnerabilities and their level of severity, and specific high risk vulnerabilities found on the network. These reports are then communicated through email to the IT Director. The evaluations performed by internal HWCOM staff did not formally document their findings, remediation options or recommendations.

The frequency of evaluations performed should take into account the sensitivity, size, and complexity of data reviewed including recent environmental, operational, and any relevant changes in regulations. By performing the evaluations periodically, the penetration tests can then be better adapted to include these changes. The frequency of evaluations performed by HWCOM internal staff has not been established.

Although the Information Technology Security Office provides adequate network vulnerability detection to the College of Medicine, the lack of periodic formal evaluations by the HWCOM internal staff and the brevity of the consultant security training session reduce the effectiveness of the established controls to respond to environmental or operational changes.

McAfee antivirus On-Access Scanner (OAS) and Microsoft Malicious Software Removal Tool are utilized to minimize the risk that workstations become infected with malware. McAfee's OAS service scans files prior to the user opening them to ensure they are not infected. The Microsoft Malicious Software Removal Tool is an anti-malware utility that checks computers running Windows operating systems for infections by specific, prevalent malicious software and helps remove malware and any other infections found.

An antivirus program blocks malicious software from running on a computer, whereas Microsoft Malicious Software Removal Tool removes malicious software from a workstation already infected. University Technology Services (UTS) manages these applications and should ensure they are updated on a daily and monthly basis, respectively.

Virus signature definition files need to be current for antivirus mechanisms to be effective. These definitions should be updated whenever new releases are available. All workstations tested were adequately configured to automatically update their virus definitions at 5pm daily. All 10 workstations tested had McAfee's OAS service actively running. Review of the OAS logs indicated that three workstations were not running with OAS enabled for part of the review period. Workstation security effectiveness is reduced when OAS is disabled. Workstations belonging to the database administrator and web developer had 47 and 120 viruses detected on their workstations, respectively.

Recommendations:

College of Medicine's IT Department should:	
1.1	Formally identify which information systems store or transmit protected data, which systems are critical to operations, and the names of the system owners.
1.2	Conduct and document a risk assessment utilizing appropriate frameworks and guidelines.
1.3	Work with other staff having security expertise to conduct periodic evaluations. The frequency of evaluations should take into account the sensitivity of the data, its size, complexity, and environmental, operational, and relevant changes in regulations.
1.4	Formally document the frequency of internal evaluations, including interviews, surveys, automated tools, system logs, penetration test results, evaluation findings, and remediation actions, including known gaps between identified risks and mitigating security controls and the justification for accepted risks.
1.5	Work with the Information Technology Security Office to ensure the two identified workstations were not breached and are adequately cleared of all detected viruses.
1.6	Periodically review OAS log files to ensure OAS is appropriately enabled and virus definitions are updated timely.

Management Response/Action Plan:

1.1 While not formally documented at the time of the audit, the HWCOM IT staff was knowledgeable of which servers/appliances contained sensitive data, which were critical to the operation and the system owners. Subsequent to the audit, the inventory report of servers has been updated and completed as of 8/15/2012 to include additional columns to identify: servers containing PHI/PII/FERPA

information, servers critical to the operation, and system owners. The methodology used to confirm the nature of the data contained on each server included: identification of each application and database by programmer, database administrator and users; evaluation of data elements within each application and database by the IT team for sensitive data.

Implementation date: Immediately

1.2 Prior to the audit HWCOM conducted informally documented risk assessments. As of August 2012, formally documented risk assessments have commenced using NIST standards for the following systems: Mobile Health Center, NeighborhoodHELP Portal, COMBACKUP and SHAREPOINT. HWCOM will continue to conduct ongoing formal risk assessments using appropriate frameworks and guidelines for systems containing sensitive data.

Implementation date: Immediately

1.3 During the audit period, HWCOM hired an Information Security Engineer. HWCOM plans to complete a risk assessment on each application or service site prior to its implementation. In addition, HWCOM has scheduled a follow up review of each application and or site at least every two years. The frequency of the review will be formally noted and included in the initial assessment. For example, a recently completed review of the NeighborhoodHELP mobile center is due to be re-evaluated in May 2014.

Implementation date: Immediately

1.4 Subsequent to the audit, HWCOM IT has developed a Security Scan Report Log to capture frequency of assessment, vulnerabilities and remediation efforts as of August 2012. The HWCOM IT Security Engineer performs a weekly review and assessment of the security scans.

Implementation date: Immediately

1.5 Both workstations were scanned by HWCOM IT Security Engineer in August 2012. Furthermore, these workstations did not appear for critical vulnerabilities in the Security Scan Report provided by FIU IT Security Office; both workstations were cleared of viruses.

Implementation date: Immediately

1.6 OAS logs are reviewed periodically by HWCOM IT Security Engineer to verify that versions are current and to assess vulnerabilities. Formal documentation of the activity started in August 2012. As noted in Item 1.4, Log Reports have been developed to capture frequency of assessment and remediation efforts.

Implementation date: Immediately

(page intentionally left blank)

B. Manage Human Resources

According to COBIT APO01.02.01, APO07.02.03, and APO07.01.03, policies and procedures should ensure that IT-related roles and responsibilities are in alignment with business needs; expedient actions are taken regarding terminations, and that background checks are performed as part of the recruitment process.

Listing necessary skills and abilities necessary to fulfill established jobs and their accompanying roles are part of the hiring process. College of Medicine's job descriptions include college degree minimum qualification requirements, departmental preferences, and specific job duties. Over 91% of those fields examined were appropriately filled-in for the 9 IT positions tested.

The College of Medicine's network systems administrators have access to the entire HWCOM network including stored protected data. This includes the Director of IT, Senior Computer Support Specialist, IT Security, Systems Support Specialist, and Systems Administrator. Examination of the job descriptions indicate that only the Systems Support Specialist and Systems Administrator duties justify their access to protected data based on the server support operations they are required to perform.

Criminal background checks are required by FIU Policy 1710.257 where a positive "clear" result ensures that appropriate screening and clearance is performed for those who will have access to protected data. This reduces the exposure to potential fraudulent behavior and mitigates the risk of inappropriate disclosure of protected data. 8 of 9 IT staff members examined had a background check performed. A background check of the IT Director was not evident, which otherwise is required due to his/her access to protected data.

The College of Medicine's Human Resource Department utilizes a separation of employment checklist to document separation notification procedures. The notification process includes the employee's supervisor, UTS, and Employee and Labor Relations (ELR) Departments. Separation procedures should entail recovery of access control devices, such as ID access cards and computer equipment, along with ensuring user access is disabled.

Twenty-two terminated employees examined had corresponding checklists. Twelve checklists were created after the employee's effective date of termination. On average, these checklists were created 12 days after the separation date. There were two checklists created 28 and 75 days after the effective date. Six of the twenty-two former employees are still enabled in the Active Directory. Disabling terminated user accounts is handled by the UTS. Some checklists did not clearly indicate that badge/ID's were collected upon separation. Two of the terminations examined had copy accounts which were created by UTS as part of internal investigations. These two accounts were still active.

Based on COBIT APO07.03.05, continuous training programs should be developed based on organizational requirements and include ethical conduct. For HIPAA related

processes, training should provide staff with the knowledge on how to guard against, detect and report malicious software, monitor log-in attempts, report discrepancies and how to create, change, and safeguard passwords. Training should be scheduled and conducted according to policy. Dissemination methods should include newsletters, screen savers, videotapes, email messages, teleconferencing, staff meetings, and computer based training. Refresher training should be performed periodically to keep the employees updated on security awareness. The security awareness training program should be kept current. Monitoring techniques should be implemented to ensure that all employees participate.

A continuous security awareness training process has not been implemented by the College of Medicine. Implementing a continuous security awareness training program will decrease the likelihood of unauthorized disclosure of protected data.

Recommendations:

College of Medicine's IT Department should:	
1.7	Reevaluate and adjust, as deemed necessary, user account access permissions for protected data.
1.8	Work with HR on the completion of a background check on the Director of IT.
1.9	Periodically review terminated user accounts to ensure they have all been disabled in the active directory and obtain confirmation that terminated employees' access has been disabled.
1.10	Ensure separation of employment checklists clearly reflect items collected from terminated employees and are completed in a timely manner.
1.11	Work with Human Resources Department to ensure that copy accounts are disabled in a timely manner.
1.12	Develop and implement a security awareness training program. The program should be periodically evaluated to ensure it is up to date and effective.

Management Response/Action Plan:

1.7 Historically, the process of assigning access permissions for protected data was based on the request of the authorized person within the department. Formal and documented process to be developed by December 2012 to re-evaluate and adjust user account access for protected data.

Implementation date: December 2012

1.8 This recommendation was completed in August 2012.

Implementation date: Immediately

1.9 Process has been established with HWCOM HR to ensure terminated employees' access have been disabled. We will obtain monthly reports of employee termination status and will verify this information against Active Directory. As FIU's Division of IT manages the termination of accounts in Active Directory, HWCOM IT will work with central IT to verify completion on a regular schedule.

Implementation date: Immediately

1.10 HWCOM HR now utilizes one standardized separation of employment checklist to reflect items collected from all terminated employees as of June 2011.

Implementation date: Immediately

1.11 Procedure has been established using a checklist for ensuring copy accounts are disabled in a timely manner, as of September 2012.

Implementation date: Immediately

1.12 There are several mechanisms for providing security training to FIU staff that are part of the FIU's covered health care components (including HWCOM and its component parts):

- University Compliance Office conducts university training for workforce members inclusive of security awareness and security strategies;
- Prior to the issuance of HWCOM owned mobile devices, workforce members undergo a HIPAA briefing;
- IT creates and distributes security awareness tips;
- Subsequent to the audit time period:
  - Focused training has been provided to workforce members who have access to ePHI.
  - Security reminders contained within the AHC FIU HCN quarterly Compliance and Quality Newsletter.

HWCOM IT Security will continue to develop a HIPAA security awareness plan to work in conjunction with UTS' Security awareness training, which is anticipated to be offered to all FIU HWCOM staff by the end of 2012.

Implementation date: December 2012

C. Manage Continuity

According to COBIT DSS04, a contingency plan should be established which enables the business and IT to respond to incidents and disruptions in order to continue operations of critical business processes and required IT services. HWCOM's Continuity of Operations Plan (COOP) Safety Training for Emergency Response Liaisons (ERL) outlines how to prepare and protect personnel and property and effectively respond to threats and hazards which are most likely to impair its mission. The Departmental COOP, last updated in August 2011, contains the Plan's objectives, scope, safety training, and defined roles and responsibilities. Individuals have been assigned to maintain the Plan. Resource requirements listed in the mission critical operations and services section is partially completed.

Items missing in the COOP include testing, hardware and software restore time requirements, alternate operational methods, vendor services, and back up requirements. The lack of these items may adversely affect data recovery in the event of a disaster.

A business impact analysis enables HWCOM's IT Department to: identify activities and materials involving sensitive information which are critical to business operations; identify alternate methods to critical services or operations that support those processes; and define allowable disruption tolerances to those operations, materials, or services. The College of Medicine has not performed a business impact analysis. The absence of a business impact analysis decreases the COOP's effectiveness.

Preventive measures for defined scenarios should be designed to decrease the risk of loss of critical and sensitive data. The COOP Safety Training for Emergency Response contains preventive measures for each defined likely scenario. The College's preventive measures are practical and feasible in terms of applicability in the current environment.

A set of contingency procedures should be invoked once a disaster has been declared to minimize the impact to the affected Department. The HWCOM's COOP contains 10 high level contingency procedure descriptions, such as computer hard drive backups, unplug and cover computers, and change personal voice mail messages as its recovery strategy, which does not adequately minimize the potential impact. The COOP documentation should provide, based on business impact assessments, detailed procedures necessary to successfully enable the continuation of critical business processes and for the protection of sensitive data when operating in emergency mode, which it did not.

HWCOM has implemented a data backup infrastructure (see Figure 1) to create and maintain retrievable exact copies of its data. Data backups are kept at an offsite data recovery location. Data is duplicated through tape backups and distributed Storage Area Network[3] (SAN) devices between the MMC campus and the data recovery site.

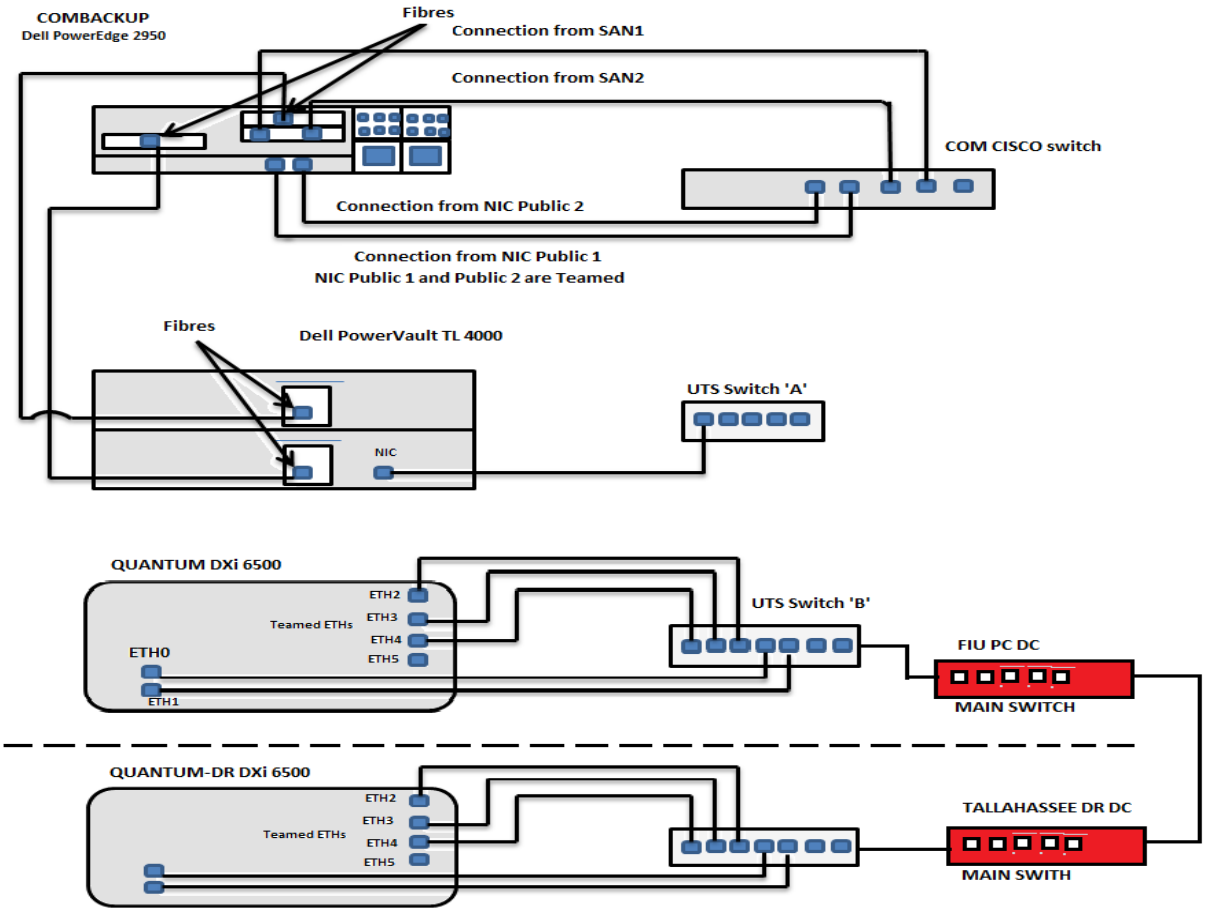


Figure 1

The redundant SAN devices are RAID[4] 50 configured which improves performance and is recommended from the manufacture for applications that require high fault tolerance capacity. Even if one drive from each of the RAID 5 sets were to fail there would be no data loss.

There are nine backup jobs scheduled for the SAN devices including daily and monthly full backups of SQL database and applications. These backup jobs are scheduled to automatically copy data between MMC and the disaster recovery site to keep exact data copies in each location.

There are also five scheduled tape backups, representing a 3rd level of backup security, which are separate from the SAN devices. Three layers of tape backups include differential, weekly, and monthly backups of all servers. Two additional tape backup

[3] An array of disk drives in a self-contained unit

[4] Redundant Array of Independent Disks

jobs are for databases and “legal”. These tape backup jobs were placed on hold and were not performed for 6 months. In addition, log files provide assurance that the backup jobs have successfully completed. HWCOM’s IT Department does not maintain or formally review backup logs.

Periodic testing of the COOP, where test findings are incorporated into the revised plan, provides assurance to HWCOM of the Plan’s readiness. Although a disaster recovery test was conducted over the weekend of July 16th and 17th, 2011, the testing was focused on web services, PantherSoft, Active Directory, and the FIU Phonebook and not on College of Medicine’s critical business processes. Additionally, key personnel should be included in disaster recovery plan testing to provide training on their roles and responsibilities in the event of a disaster. HWCOM key personnel were not included in the weekend disaster recovery testing.

In the event of a disaster, specific HWCOM IT individuals in the Continuity Plan should have building access to the information systems backup and recovery systems. The College of Medicine’s disaster recovery information systems are located outside of the IT Department. The servers and backup systems are located within the UTS Department at the MMC campus. The UTS provides the IT facility infrastructure and the College of Medicine’s IT Department maintains the equipment and the sensitive data residing on those servers. Those responsible for information systems backup and restoration do not have access to the UTS facilities. They have to contact UTS and wait to be let in. The lack of badge access to those responsible for backup and restoration may impede the College of Medicine’s disaster recovery efforts.

Disaster recovery contracts with outside vendors help ensure the success of contingency services not provided directly by the College of Medicine. Contracts should ensure that reasonable efforts are made by outside vendors to protect the confidentiality, integrity, and availability of that data, both in transit and at rest. The UTS Department is only responsible for providing the data connection infrastructure to the disaster recovery site. The College of Medicine is responsible for the server operations. A contract was drafted in December 2010 between UTS and the College of Medicine, but never executed. In its draft form, the contract is missing administrative, physical, and technical controls which will be implemented on behalf of the College of Medicine. The contract should also ensure that outside vendors report all security breaches to the College of Medicine.

Disaster recovery services are provided by a 3rd party vendor. The College of Medicine should ensure that the vendor has implemented administrative, physical, and technical controls to protect the data residing at its facilities. Periodic risk assessments and Service Organization Control (SOC) 2 reports are effective methods to ensure that the 3rd party vendor’s controls adequately protect sensitive data. The UTS Department, acting as the business continuity liaison, has not performed or requested a risk assessment be performed on the disaster recovery vendor’s site.

Recommendations:

College of Medicine should:	
1.13	Update the Continuity of Operations Plan (COOP) to include training, testing, hardware and software restore time requirements, alternate operational methods, vendor services, and back up requirements.
1.14	Perform a business impact analysis for all critical business operations.
1.15	Keep backup log files and formally review them to ensure that the backups have successfully completed.
1.16	Ensure continued service and the protection of sensitive data by performing disaster recovery testing and refine the COOP accordingly, giving due consideration to critical business operations identified in the business impact analysis; and document COOP roles and responsibilities.
1.17	Work with UTS to allow access to the data center facility in support of the restoration effort in the event of a disaster.
1.18	Work with UTS to ensure that the completed disaster recovery services provide for administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity, and availability of the data residing at the vendor's facility.
1.19	Work with UTS to consider requesting that the vendor providing disaster recovery services conduct a risk assessment or provide a Service Organization Control (SOC) 2 report to ensure that administrative, physical, and technical risks are reasonable and appropriately mitigated.

Management Response/Action Plan:

1.13 The HWCOM has implemented and documented its back up procedures including periodic testing and review of the back-up jobs. Currently, the HWCOM COOP plan undergoes yearly review but will be revised to occur bi-annually in February and August. The next revision will take place February 2013.

Implementation date: February 2013

1.14 HWCOM will conduct a business impact analysis on all critical business operations by February 2013.

Implementation date: February 2013

1.15 Backup log reviews were performed by the HWCOM Systems Administrator and Database Administrator daily; however, they were not formally documented. A checklist and comprehensive log spreadsheet has been developed as of September 2012 to formally document the log review process.

The HWCOM will continue to refine its backup and business continuity solutions in conjunction with the larger FIU community.

Implementation date: Immediately

1.16 The Disaster Recovery site is currently under development for completion. The projected plan for completion is June 2013. This effort is done in conjunction with FIU Department of IT. Plans for periodic testing of the COOP will be completed by June 2013.

Implementation date: June 2013

1.17 The current procedure for the datacenter facility as established by FIU Department of IT Operations Center requires making an appointment to enter the facility. HWCOM IT will work with the Operations Center by December 2012 to establish a more autonomous process for gaining access to HWCOM equipment in the event of a disaster, while maintaining optimal security.

Implementation date: December 2012

1.18 As part of completing the Disaster Recovery site, HWCOM IT will work with UTS to ensure appropriate safeguards protect the data at the Northwest Regional Datacenter (NWRDC) by June 2013.

Implementation date: June 2013

1.19 As mentioned in 1.16, the Disaster Recovery site is under development for completion in June 2013. As part of this process, HWCOM will work with FIU's Division of IT to conduct a risk assessment or provide a SOC 2 report to ensure reasonable protection of the confidentiality, integrity and availability of the data and services.

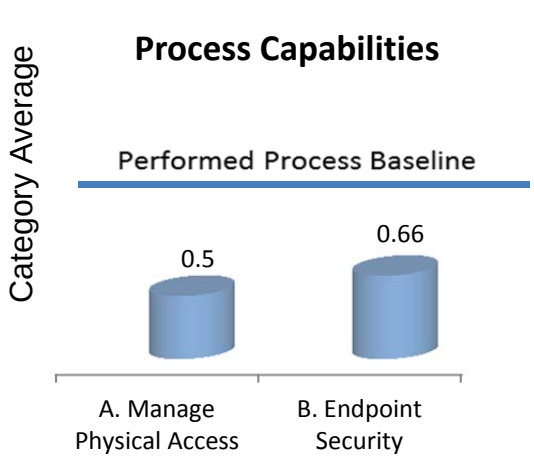
The HWCOM is part of the larger FIU backup solution. We plan to continuously improve our process as recommended by FIU's Division of IT, the Department of Emergency Management and any appropriate FIU governing body.

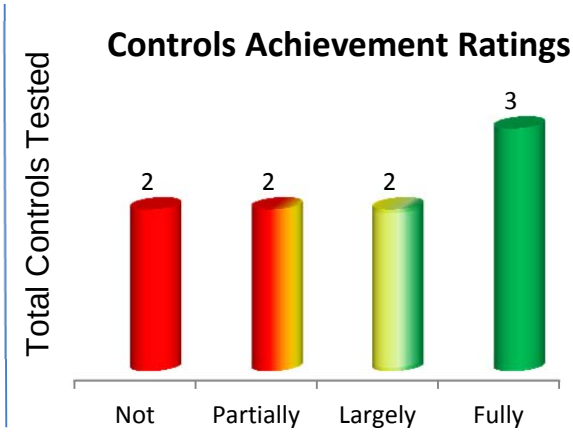
Implementation date: June 2013

(page intentionally left blank)

2. Physical Controls

Physical Controls are the physical measures, policies, and procedures to protect an entity's electronic information systems and related buildings and equipment from natural or environmental hazards, unauthorized intrusion, and proper disposal of sensitive data when no longer in use.





We tested two areas within the Physical Controls and found that 4 of the 9 control activities selected need improvement to ensure that they meet their objectives. Overall, Physical Access controls need improvements in operating the building access application. Duplicate room access capability between the on-line application's user groups reduces their effectiveness to control room access. The large amount of users with access to the HWCOM IT Department highlights the need to improve Physical Access controls. There is a security gap in the way the on-line building application handles group profiles which increases the risk of unauthorized building access.

HWCOM's IT Department adequately maintains accountability on equipment that is has issued for both business-related computers and student tablets. However, the ITSO Media Sanitization Department should formalize its hard drive eraser procedures to improve its Endpoint Security controls. The lack of formal documentation for all sanitized hard drives by the ITSO Media Sanitization Department increases the risk that sensitive data is inappropriately exposed.

A. Manage Physical Access

According to COBIT DSS05.05, physical access should be defined and implemented to grant, limit, and revoke access to premises according to business needs. Access to premises should be justified, authorized, logged and monitored.

In December 2011, the University's Department of Research and Key Control met with members of HWCOM to discuss building security and the protection of researchers during off hours. The meeting identified vulnerabilities, specific shortfalls, and potential

improvements to existing mitigating controls. As a result of the meeting, the College of Medicine had all perimeter doors converted to the on-line card access system.

Access point entryway controls are implemented to limit access to HWCOM's IT Department's equipment. The main entrance has a dual door entry system. The first door requires a card swipe and the second "inner" door is key-locked, which can be overridden by an electronic bypass system. The second "inner" door and the side hallway share the same physical key configuration. All nine IT employees tested have proper/justifiable access.

Obtaining access to the IT Department should follow an established process based on employees' job duties. There were 81 individuals with active badge access to the IT Department, representing an excessive number of users. We tested the requests for 36 active badges and found that: 20 user accounts were granted to individuals outside the HWCOM, e.g., Facilities, General Counsel, etc.; 2 user accounts were for a subsequently terminated employee; and 1 was issued without a valid user ID.

The badge activation process is not consistently applied. Approximately 75% of the email requests tested went to Key Control and the balance sent to the College of Medicine's Administrator user group. 13 user accounts requesting access to the IT Department were examined. 12 email requests came directly from the IT Director, with 8 going to Key Control and 4 to the Administrator user group. One was directly sent from an employee to the wrong individual and was then appropriately redirected.

Deactivating building access should be performed in a timely manner when badge access is no longer appropriate. 3 of the 81 individuals with active door access to the IT Department were terminated employees. The HWCOM Human Resources Department does not maintain badge access records for part-time employees and it is unknown whether the one part-time employee returned their key card. The current badge deactivation process requires manual notification to the Key Control Department. Without proper notification, terminated users badge access may not be removed in a timely manner. This is evidenced by 3 terminated users remaining on the system an average of 214 days after their termination date. The risks of inappropriate building access are adequately mitigated as the 2 full-time terminated employees returned their access key.

The facilities reporting and oversight process for the College of Medicine is sectioned into four separate user groups which covers the Academic Health Center I, II, and Owa Ehan buildings located on the MMC campus. Each user group provides badge access to selected rooms and buildings.

All group administrators are required to sign the Key Control Department's acceptable use procedure forms to ensure they understand their roles and responsibilities. There are a total of six group administrators for the four user groups. Four of five group administrators signed the acceptable use form and one is a test account. The four user groups are:

- Group 1 is the Administrator group which is controlled by the College of Medicine's Chief of Staff. The Administrator group manages access to 43 entryways in the Academic Health Center II building including the IT Department. Only the Facilities Department and the Administrator group are able to manage access to the IT Department.

- Group 2, Office of Research group, is controlled by the Assistant Director of Research Programs and is responsible for 25 entryways located on the 3rd and 4th floors of the Academic Health Center I and a part of the Owa Ehan building's 3rd floor.

- Group 3 is the OME group which is controlled by the Assistant Director of Medical Education, Administrative Assistant and a test account. The OME group controls the classroom and study room access to 36 entryways in the Academic Health Center II building. These entryways are shared with the Administrator and Student Affairs user groups.

- Group 4, Student Affairs group, is controlled by the Director of Administration and the Assistant Director of Administration Operations. They are responsible for classroom access for 34 entryways in the Academic Health Center II building.

Through the on-line access application's profile, access is segregated in such a way so that group administrators can only see users that they grant building access to. With a lack of detailed building access reports available, managing building access becomes problematic in the Academic Health Center II building. On average, 88% of the entryways are duplicated between the Administrator, OME and Student Affairs user groups. These groups cannot see a complete list of users to rooms which they are responsible for and are unable to properly administer building access.

Badge access audit trail reports that detail building usage should be reviewed for violations, abnormalities, and prioritized by location sensitivity. These audit trail reports would help the College of Medicine group administrators identify outliers and alert to potential violations of building access. Badge audit trail reports are not available to group administrators. The unavailability of room usage reports and their lack of review increase the risk of inappropriate access.

Computer supplies are stored in a supply room located within the IT Department location. The supply room has a physical key lock to safeguard the stored equipment controlled by the IT Director. However, we observed that the main entryway while activated, was left ajar and both the storage room and side hallway entry were unlocked.

Recommendations:

College of Medicine should:	
2.1	Review and reorganize user groups and their related administrators based on logical access requirements.
2.2	Ensure terminated employees' badge access is appropriately disabled and access to IT Department is appropriate.
2.3	Provide Key Control with all acceptable use procedure forms.
2.4	Request that Key Control remove or deactivate their test account.
2.5	Periodically review badge access reports to ensure access is appropriate.

Management Response/Action Plan:

2.1 - 2.5 HWCOM is working on a security access process to centralize all key access and controls under the HWCOM Finance and Administration Office, specifically under the Director of Facilities Operations. This process will formalize all procedures regarding badge access and key control which cover the entire spectrum of providing access and disabling access. This process is on-going and will be finalized and tested by December 2012.

Implementation date: December 2012

B. Manage Endpoint Security

According to COBIT DSS05.03.09, DSS05.06.03, and DSS05.06.05, HWCOM should ensure endpoint devices, such as laptops and other mobile devices are protected, inventoried, and any sensitive data is properly disposed of when no longer in use.

The College of Medicine utilizes spreadsheets to maintain accountability on equipment issued on 435 business-related computers and 179 student tablets. These spreadsheets adequately track the movement of these items within the facility and who is accountable for the equipment by documenting the user name, host name, MAC[5] address, and service tag number.

When computers reach their end of life or are no longer in service, formal policies and procedures governing device and media controls activities ensure they appropriately address the final disposition of hardware or electronic media on which sensitive data is stored. While the Information Technology Security Office does not have formal policies and procedures, media sanitization reports are issued from their Media Sanitization Department when they erase hard drives.

The media sanitization procedures should wipe previously stored sensitive data on electronic media to ensure it cannot be accessed or reused. During the review period, two former students' tablets were sent to the Media Sanitization Department to erase all data off of their hard drives. The tablets were returned to the College of Medicine minus the original hard drives. As an extra safety precaution, the hard drives were degaussed which destroys the hard drive and renders the hard drive inoperable. This process ensures the student's tablet data could not be accessed or reused.

When erasing a hard drive, it is the responsibility of the Information Technology Security Office's Media Sanitization Engineer to record the receipt and removal of hardware and software containing sensitive data from storage devices. The above tablets' hard drives were not formally documented. For hard drives that are not degaussed, the lack of formal media sanitization documentation may increase the risk of inadvertently releasing or sharing of sensitive data with an unauthorized party.

[5] Media Access Control is an ID that is assigned to any device with networking capabilities

Recommendations:

Information Technology Security Office should:	
2.6	Formally document media sanitization policies and procedures to govern the receipt, use, removal, and disposal of College of Medicine's information systems.
2.7	Formally record the receipt and removal of the two tablets' hard drives.

Management Response/Action Plan:

2.6 Media sanitization policies and procedures have been completed and can be found at http://security.fiu.edu/Pages/mediasan.aspx.

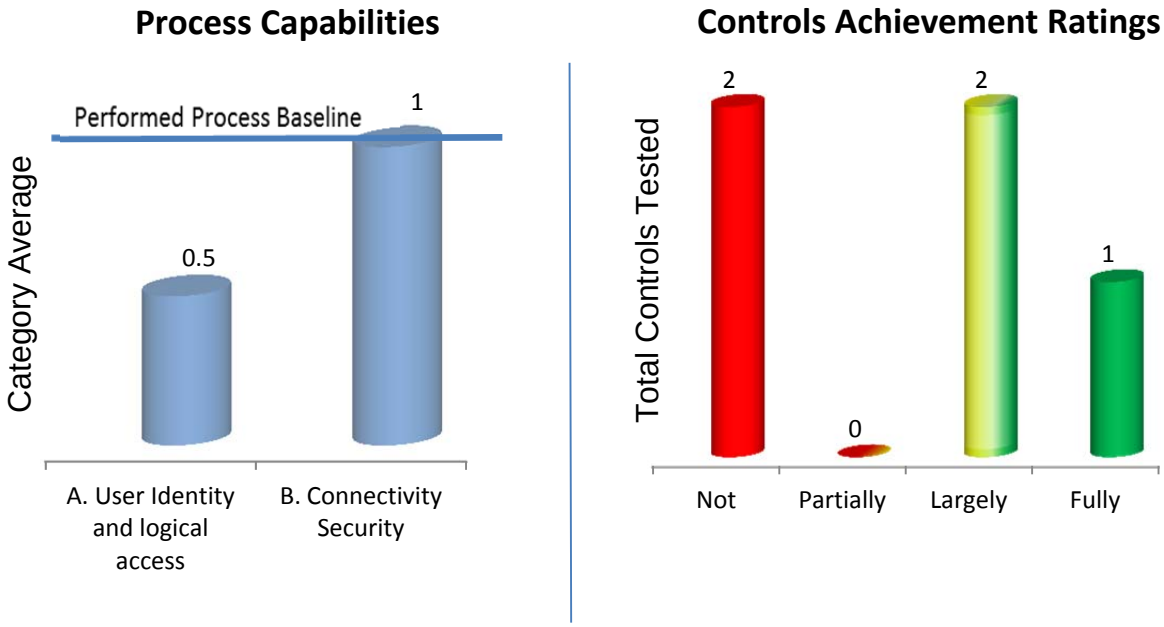
Implementation date: Immediately

2.7 We have completed this. Future procedure will include the issuance of a Chain of Custody Form from the ITSO.

Implementation date: Immediately

3. Technical Controls

Technical Controls are the technology policy and procedures implemented that protect sensitive information and control access to it.



We tested two areas within Technical Controls and found that 2 of the 5 control activities selected need improvement to ensure that they meet their objectives. Overall, User Identity and logical access controls need some improvements in reducing the amount of administrators, disabling terminated users, and removing non-unique user accounts within workstations, applications and databases. The informal manner in which users are created contributes to inappropriate user access and should be in accordance with their business function and process requirements. Account identities and their access rights should be based on least-privilege, need-to-have and need-to-know principles.

There is evidence of audit trails which record user actions including account creation, modification, and who performed the activity. The lack of a formal review of these logs reduces the effectiveness of these audit trails as an audit control. Online data is adequately encrypted in transit and is an effective Connectivity Security control.

A. Manage User Identity and Logical Access

According to COBIT DSS05.04.07, DSS05.04.08, and DSS05.07.03, policies and procedures should be implemented to ensure all users are identifiable, an audit trail tracking access to information classified as highly sensitive, and that the audit trails are reviewed for potential incidents. Access controls for HWCOM IT workstations and software applications DOME, Titanium, and Neighborhood Portal, were selected for testing. These three applications were selected for testing due to the sensitivity of the

data that they store. Potential financial impact calculations of $112 per record affected are based on the Ponemon 2010 Annual Study of U.S. Cost of a Data Breach[6] for the education industry.

I. Workstations

Administrator accounts are inherently risky due to the elevated access privileges which are associated with these users. Assigning unique identities to administrator accounts enables individual users to be identified and their activities tracked. For nine of the ten workstations examined there were three main user group accounts and one attached user group with administrator access. Within these administrator user groups, there were 81 uniquely identifiable user accounts. This number of user accounts for just nine workstations is deemed to be excessive. This is caused by the inherit properties of active directory groups where different user groups are assigned to these workstations. User accounts which are not uniquely identifiable include two system accounts; two ITSO accounts; one helpdesk account; and two non-active directory user accounts which may be used as a shared user account to these workstations.

II. Titanium Application

The Titanium application is used by the Counseling and Wellness Department. Due to the data sensitivity of the 101 student accounts, the potential impact financial to HWCOM could total $11,312. According to the Director of Counseling and Wellness, Titanium which has been used since the College's inception, is accepted by clinical psychologists nationwide because of its security and application capability. The application is used by staff members to set student appointments, document sessions, and record psychological evaluations.

Within the application, there are a total of six active staff user accounts with five uniquely identifiable and one non-unique user account. The application administrator was uncertain as to how many total administrators there are for the application.

There are seven individual user accounts to the Titanium database. These are connections that connect directly to the database and are not controlled by the Titanium application. Four of seven database connections are uniquely identifiable. One of the four database accounts is for the Director of Counseling and Wellness and can be used to bypass Titanium's user access controls. Two of the remaining three user accounts that are not uniquely identifiable have database owner access privileges.

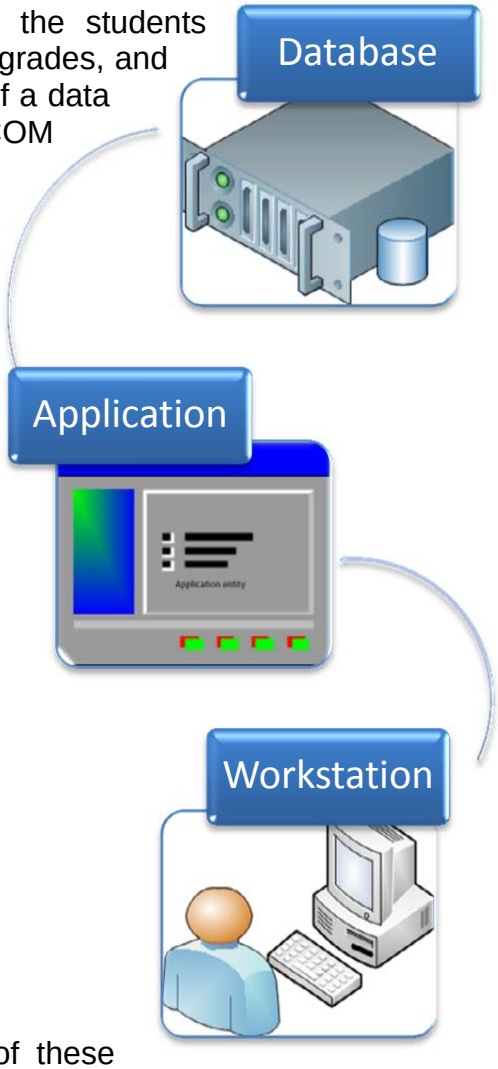
At the database server level, where the Titanium database resides, there are 15 active user accounts. 12 of the 15 user accounts are uniquely identifiable. The remaining three

[6] The 2010 Ponemon Institute benchmark study, sponsored by Symantec Corporation, examined the cost incurred by 51 organizations after experiencing a data breach. Results represent direct and indirect cost estimates for activities resulting from actual data loss incidents. Breaches of the 51 organizations who responded to the annual study ranged from 4,200 records to 105,000 records from 15 different industry sectors. These costs estimates are used to calculate potential impact only as actual costs may vary.

user accounts are non-identifiable. The non-identifiable accounts have a greater risk because these accounts are at the database server level and could be used as shared accounts and actions performed would not be tracked back to an individual user account.

III. Data Organization for Medical Education (DOME) Application

The Data Organization for Medical Education (DOME) is an admissions portal used by students and the Office of Student Affairs. Students submit their information when applying to the College of Medicine. There are 9,121 student accounts in the DOME database. The data that the students transmit includes personally identifiable information, grades, and credit card number and CVV2[7] codes. In the event of a data breach, a potential impact of $1,021,552 to HWCOM could result due to the sensitivity of the data stored.



There are a total of 171 active staff user accounts which are uniquely identifiable on the DOME application program. One of the active accounts is a consultant who is no longer providing services to the DOME application. There is also one non-identifiable guest account that is not active. We observed that during the account creation process, an email disclosed seven individual user's username and password. According to FIU Policy 1930.020b, individual access codes should be kept confidential and not be disclosed. This email was sent to the application's supervisor as confirmation that these accounts were created. The information enclosed in the email potentially exposed those user accounts and the data they are able to view to unauthorized use.

The application server where the DOME application resides has 19 individual and 6 non-identifiable active user accounts with administrator privileges. 6 of the 19 individual user accounts are used for testing purposes. It is not a "good practice" to have active test accounts on production servers. One of these user accounts is a consultant who is no longer providing services to the DOME application.

The DOME database has no unique users and 4 non-identifiable user accounts. Two of the four user accounts have administrator privileges. One is a guest account and the

[7] Card Verification Value

other has no privileges. The database server where the DOME database resides contains 7 unique users and three non-identifiable administrator user accounts.

IV. Neighborhood Portal Application

The Neighborhood Portal is an online application used by staff members to schedule appointments and record their patient visits. Patient medical data may be stored on select fields within the application. With the database storing sensitive data for 1,505 households, the potential financial impact to HWCOM in the amount of $168,560 could result in the event of a data breach.

There are 375 enabled staff and student user accounts uniquely identifiable on the Neighborhood Portal application, including one consultant account that is no longer providing services to the Neighborhood Portal application. There are two non-identifiable user accounts with administrator privileges.

The application server where the Neighborhood Portal resides contains: 6 individual accounts; 2 system accounts; and 1 non-identifiable user account with a non-expiring password. All of above listed user accounts have administrator privileges to the application server.

The Neighborhood Portal database has 2 non-identifying administrator user accounts, including a known generic administrator user account which was automatically created during the database installation. The database server where the Neighborhood Portal database resides has 1 non-identifiable system administrator account.

User accounts, like those listed above, should be formally created through Identity Access Management (IAM) policies which address purpose, scope, roles and responsibilities, along with legal and regulatory guidelines. Currently, there are no formal Identity Access Management policies developed or implemented for workstations or the above software applications. The lack of formal Identity Access Management policies increases the risk of inappropriate and unauthorized access to sensitive data. The inherent risks are further evidenced by 85 administrator workstation user accounts, 33 Titanium administrator users, 25 DOME administrators, 36 Neighborhood Portal user accounts with administrator privileges, and emails containing active user IDs and passwords.

V. Audit Trails

Audit trails maintain a record of information system activities which can assist in detecting security violations. An audit trail is a series of recorded events about user activities. Audit trails can help establish an individual’s actions and accountability.

Workstation user actions are recorded and stored in the event logs. However, workstation event logs are not periodically reviewed.

The Titanium application records the workstation's hostname that the user logged in with, successful and failed user logins, the date time a user logs in, and the individual's active directory user ID. While there were 4,516 additional audit log entries detailing user activities, once they are in the system the application's administrator does not know how to obtain that information and has requested help from the vendor.

DOME and the Neighborhood Portal audit logs record the date that user accounts are created or modified and who performed these actions. Neighborhood Portal audit logs also record when field data have been created and updated. None of the log documentation provided showed who viewed identified sensitive data fields.

Audit trail data should be monitored to derive exception reports. The exception reports may then be used improve internal evaluations and security controls. Audit logs reviews are not formally performed which is necessary to derive exception reports.

B. Manage Network and Connectivity Security

According to COBIT DSS05.02.04, information in transit should be encrypted based on its classification.

The Neighborhood Portal and DOME applications are web based systems that secure their data transmission through SSL[8] | TLS[9] encryption technology. Both applications use TLS 1.0 RC4_128 bit encryption with MD5[10] for message authentication and RSA[11] as the key exchange mechanism. The use of the above encryption methods adequately secures sensitive data in transit.

Direct connection to the databases requires an active VPN[12] client user account. HWCOM ensures that the user has been identified and data communication is adequately protected from being intercepted during transit.

[8] Secure Socket Layer is an encryption mechanism

[9] Transport Layer Security is an encryption mechanism

[10] Message Digest Version 5 commonly used to check data integrity

[11] RSA is an algorithm for public key cryptography

[12] Virtual Private Network requires remote users to be authenticated and make use of encryption techniques to prevent disclosure of private information to unauthorized parties present on the network that the VPN transmits data through

Recommendations:

College of Medicine should:	
3.1	Review the number of individual user accounts with workstation administrator access privileges to ensure access is appropriate.
3.2	Ensure Titanium database administrators' access is appropriate and disable the Director of Counseling and Wellness direct database account.
3.3	Disable DOME active consultant and test accounts on production servers.
3.4	Ensure that the list of Neighborhood Application Server Administrator members are appropriate; remove the consultant and default non-expiring account from Neighborhood Portal application and database server, respectively.
3.5	Review non-identifiable user accounts to determine if they can be appropriately identified and monitored.
3.6	Document Identity Access Management policies.
3.7	Develop and implement a formal audit log review process.
3.8	If feasible, update log capability to include automatic notification and when users view sensitive data fields.

Management Response/Action Plan:

3.1 The HWCOM workstations are jointly managed by HWCOM IT and FIU DoIT. The workstations are joined to DoIT's Active Directory infrastructure. As such our workstations inherit Group Policies created by both DoIT and HWCOM IT. Part of the Group Policy includes AD user group accounts that are added to the workstations for management purposes. These user groups include both service accounts and individual member accounts. HWCOM will work with UTS to review AD user groups added to the workstations by December 2012.

Implementation date: December 2012

3.2 HWCOM has evaluated the database and has:

- Determined the administrator's access is appropriate as the user administers new user accounts and is the super user of the application.
- Disabled the former Director of Counseling and Wellness database account.

Implementation date: Immediately

3.3 HWCOM has evaluated the database and has disabled the consultant's account on 8/17/2012.

Implementation date: Immediately

3.4 The current server administrators for the NeighborhoodHELP Application and Database servers are the appropriate members. The consultant account has been removed. The default non-expiring account is the local Built-In Administrator, which has already been disabled.

Implementation date: Immediately

3.5 The two "non-identifiable accounts" are identified as: 1) The Built-In Local Administrator account, which is appropriately renamed and disabled, 2) A system default SQL Database, dbo user. This is a system account and cannot be renamed.

Implementation date: Immediately

3.6 Formal policies for Identify Access Management will be developed by January 2013.

Implementation date: January 2013

3.7 Although not formally documented, HWCOM has been conducting periodic and ongoing audits of the databases and applications that contain ePHI as well as those that do not. This process will be formalized in a procedure by December 2012.

Implementation date: December 2012

3.8 HWCOM will research appropriate solutions that would allow automatic notification when users view sensitive data fields. Such solution will be implemented if it is feasible. Research will be completed by June 2013.

Implementation date: June 2013