2008 Information Systems Audit Reports Released Since Last Meeting by the North Carolina Office of the State Auditor:

1. East Carolina University: – (Information Systems Audit Review): Four Audit Findings

   Report URL:
   http://www.ncauditor.net/EpsWeb/Reports/Infosystems/ISA-2009-6065.pdf
   See Attachment

ECU Information Systems Audit Report Findings and Responses

The following audit results reflect the areas where ECU has performed satisfactorily and where recommendations have been made for improvement.

GENERAL SECURITY ISSUES

General security issues involve the maintenance of a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, proper segregation of duties, a security organization and resources, policies regarding access to the computer systems and a security education program. ECU has established a reasonable security program that addresses the general security of information resources. *Our audit identified one significant weakness in general security.*

AUDIT FINDING 1: ECU DOES NOT HAVE A CURRENT RISK ASSESSMENT

Although East Carolina University provided documentation to show that they performed a business risk assessment, we found that this assessment was outdated and did not include the critical Banner application. The University should maintain a current business risk assessment to identify, evaluate, and prioritize business risks which could significantly impact the university. A risk assessment allows the University to place preventive measures in their environment to reduce the risk of loss or irregularities and to ensure that the critical areas remain effective.

COBIT PO9.1 Business Risk Assessment states that management should establish a systematic risk assessment framework. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. The policy should mirror the business objectives and focus on the minimization of risks through preventive measures.

Recommendation: ECU's management should adopt a set of formal standards to ensure that critical information security elements are included and kept current in their business risk assessment.

Auditee's Response: The University agrees that in order to achieve effective Information Security governance, a Business Risk Assessment must be performed. The Chief Information Officer (CIO) will initiate a process to accomplish this.

The University is committed to managing the risks to the University's information to an acceptable level to support the achievement of the University's business objectives. The University has transitioned from a mainframe-centric administrative system to a Banner ERP system. Changes to IT infrastructure, hardware, software, processes, procedures and personnel necessitated extensive changes to IT operations. Integrated into these changes were security measures which ensured information security risks were mitigated and potential threats were reduced to an acceptable level. Although ECU has not formally conducted a current Business Risk Assessment, we have identified critical IT resources, threats, vulnerabilities, risk exposure and impact of potential compromises. In an effort to minimize threats and vulnerabilities, ECU has implemented programs that form a sound security management structure. Such programs as the Information Security Policy Suite, Security Training and Awareness Program, Data Classification and Ownership System, Hardware Asset Management Program, IT Change Management Program, Systems Planning Committee, Request for Software Services Program, Identity Theft Protection Program, a stellar Disaster Recovery Program, Award Winning Data Backup and Storage Program and the new Enterprise Risk Management Team reflect our commitment to information security.

ACCESS CONTROLS

The most important information security safeguard that ECU has is its access controls. The access controls environment consists of ECU's access control software and information security policies and procedures. An individual or a group with responsibility for security administration should develop information security policies, perform account administration functions and establish procedures to monitor and report any security violations. *Our audit identified several significant weaknesses in access controls. Due to the sensitive nature of some of the conditions found, we have conveyed these findings to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18). Our audit also identified a significant weakness in access controls over the network wiring closets.*

AUDIT FINDING 2: ACCESS TO NETWORK WIRING CLOSETS

Various wiring closets throughout ECU's campus were not secure and/or contained debris, boxes, chemicals, and other items. In a defense-in-depth security model, wiring closets have been identified as one of the most vulnerable and overlooked components in security. Securing wiring closets can be difficult since their locations are often outside of a centralized server room. However, this vulnerability can provide physical access to critical networks, and essentially bypasses all logical access controls implemented to prevent data flow interruption or corruption of data. Given the high threat level that an improperly secured wiring closet can pose, it is critical that entities take steps to physically secure them in the same manner as the main computing center.

ISO/IEC 27001:2005, A.9.2.3 (Cabling Security) states that power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. Additionally, ISO/IEC 27001:2005, A.9.2.1 (Supporting Utilities) states that equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Recommendation: ECU should ensure all wiring closets are properly secured and are free from debris.

Auditee's Response: The University concurs with the need to secure the communications closets. Information Technology and Computing Services (ITCS) will take the required actions. The closets identified by OSA as not meeting current standards are located in older buildings or leased buildings where dedicated secure space was unavailable. Secure management of these shared spaces has long been an issue for a variety of reasons including lack of awareness of responsibilities by other closet users and by building managers. As buildings are renovated, dedicated secure space is utilized for the communications closets. The University's newer closets reflect a fully controlled environment and the OSA conclusions reflect this.

As a compensating control, the shared access closets are protected via network port lockdown commands. This is done on the specific switches where there is a likelihood of physical access to the network switch.

The University will set up a formal procedure for periodic closet review for items listed in this finding.

SYSTEMS SOFTWARE

Systems software is the collection of programs that the computer center uses to run the computer and support the application systems. This software includes the operating system, utility programs, compilers, database management systems and other programs. The systems programmers have responsibility for the installation and testing of upgrades to the system software when received. Systems software changes should be properly documented and approved. *Our audit did identify a significant weakness in system software.*

AUDIT FINDING 3: PATCH MANAGEMENT PROCEDURES ARE INCOMPLETE

We noted the following weaknesses in our review of System Software:

1) The Change Management Procedures are incomplete with respect to system software changes/upgrades and do not contain the following:

    a) Test procedures for software implementation and review and approval procedures for test results

    b) Performing changes (should be system programmers only)

    c) Documenting problems and resolutions occurring during system changes

    d) System software changes are made when they are least likely to negatively impact production

    e) A written procedure is in place for testing changes to system software

    f) Problems occurring during testing are resolved and retested

    g) Test procedures are adequate to provide reasonable assurance

    h) Fallback or restoration procedures are in place in case of unforeseen problem with an upgrade or modification

    i) Each change is tested before implementation

j) Proper approval is obtained before implementation

k) Programmers maintain detailed documentation of all changes, testing, results, approvals and move to production.

2) Systems Administrators have not installed critical patches on the critical operating systems in a timely manner. Security patches are released by the operating system vendor to fix vulnerabilities and correct errors in the systems. We found the University has not installed the latest majority of security patches for the operating system as recommended by the vendor. Failure to install patches timely increases the risk that someone can exploit the vulnerabilities that would have been fixed by the patch. This could allow unauthorized access into the University's critical systems. Operating systems patches were last applied in November and December of 2007.

COBIT DS5.9 Malicious Software Prevention, Detection and Correction states that management should ensure that preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (viruses, worms, spyware, spam, internally developed fraudulent software, etc.)."

Recommendation: The University should implement procedures to adequately document their patch management program, and they should also develop a procedure to install security patches to critical systems on a regular basis.

Auditee's Response: This response is in two parts based on the two elements of the recommendation. ITCS will take the required actions.

1. <u>Documentation of patch management program:</u> The University concurs with this finding. The University has a comprehensive change management (CM) program, which we will document in the form of specific policies/procedures.

   The majority of the steps outlined in the OSA finding are practiced in ECU's Change Management Committee (CMC) for any software system changes that affect our "Production" systems and are outlined in the supporting documentation that was submitted to OSA. The CMC meets weekly to review and approve every system software change request and the CM documentation provided detailed the tracking, review, approval, implementation and fallback or restoration plans.

2. <u>Installation of security patches in a timely manner:</u> The University concurs with this finding. The University makes every effort to balance the need between system security and system availability, particularly given the heightened expectation of 24x7 Banner availability by end users. Operating system patches require downtime to apply, some requiring reconfiguration reboots. The UNIX team attempts to limit the impact on the users as much as possible. By first reviewing the system changes which will be made by each patch, then testing each patch on less critical systems for at least two weeks (SUN recommends 30 days) before applying them to critical systems, and finally applying the patches as a group or cluster of patches to reduce downtime. Our

current maintenance window is on Sundays between 5:00 am and 12:00 noon, and is shared by Applications, Database, Networking, and Storage teams. The bi-yearly patch frequency is a direct result of the business availability requirements, shared maintenance window and the time needed to research/test patches prior to deploying to all of our production systems. ECU is currently working with the functional units to pre-determine one day each month where the Banner systems could be available for maintenance. We will continue to work with the business units, senior management and the Change Management Committee to request more frequent maintenance windows be made available for system patching.

SYSTEMS DEVELOPMENT

Systems development includes the creation of new application systems by development or acquisition or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the agency in significant ways. Consequently, the agency should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include a comprehensive set of documentation so that the users, operators and programmers each have the information they need to do their jobs. *Our audit did not identify any significant weaknesses in systems development.*

PROGRAM MAINTENANCE

Program maintenance consists of making changes to existing application systems. Programmers should follow program change procedures to ensure that changes are authorized, made according to specifications, properly tested, and thoroughly documented. Application programmers should be restricted to a test environment to ensure that all changes to production resources are tested and approved before moving the changes into production. Changes to application system production programs should be logged and monitored by management. *Our audit identified one significant weakness in program maintenance.*

AUDIT FINDING 4: NONCOMPLIANCE WITH PROGRAM CHANGE CONTROL POLICIES

All program changes are required to go through the Request For Services (RFS) system. ECU did not follow current program change control policies nor could they provide adequate program change documentation to support the program changes tested under this review. More specifically, complete documentation did not exist to support who requested, made, tested, implemented and approved the program changes. These program changes did not go through the RFS system.

Lack of policy enforcement, specifically with regard to segregation of duties and documentation standards in the program change process contributed to this condition. Documented segregation of duties between the person who makes the program change and the person who approves the change helps to ensure that changes are warranted and authorized. Also, proper documentation throughout the program change process enhances the quality control measures implemented in the change management process. The lack of segregation of duties and proper documentation increases the risk that the integrity of the changed application is compromised.

COBIT AI6 states that "Control over all changes, including emergency maintenance and patches relating to infrastructure and applications within the production environment, should be formally managed in a controlled manner. Changes (including those to procedures, processes, and system and service parameters) should be logged, assessed and authorized prior to implementation and reviewed against planning outcomes following implementation."

Recommendation: Management should enforce its policies and procedures for program changes made to the application software. Also, management should require that the current RFS system be used for ALL changes to its applications so that proper documentation can be maintained, and this information be retained for a period of at least three years or until audited.

Auditee's Response: The University concurs with this finding. ITCS and Systems Coordination will take the required actions for their respective program changes.

ITCS has a Request for Service (RFS) system for all application program changes, as well as documented program maintenance procedures and procedures for placing applications into Production mode. The four sample changes were atypical in that two were from ECU's Systems Coordination unit in Financial Services which is not under the direct control of ITCS and, therefore, do not fall under the purview of ITCS Software Development Services. The other two changes were emergency changes. We will ensure that ALL changes under the control of ITCS, including emergency changes, have an RFS and are implemented in accordance with our documented policies and procedures. We are in the process of implementing Microsoft's TFS (Team Foundation Server) product across all areas within ITCS Software Development. This will provide complete source control/versioning and change process management.

The Systems Coordination unit within Financial Services is separate from ITCS. Management of this unit is in the process of establishing a formal procedure for the creation and modification of scheduled production jobs that are under the purview of Financial Services. This procedure will require the functional user to submit a formal request that Systems Coordination staff will update. Documentation will be maintained to track the flow of the request from when it is initially received to when it is completed, approved, tested, and moved to production. Systems Coordination will assume full responsibility for adhering to this policy. Previously, report changes and approvals were documented via email and comments inserted directly into the program files.

PHYSICAL SECURITY

Controls over physical security are designed to protect a computer center from service interruptions resulting from fire, water, electrical problems, vandalism, and other causes. ECU's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. *Our audit did not identify any significant weaknesses in physical security.*

OPERATIONS PROCEDURES

The operations of the computer center include all of the activities associated with running application systems for users. Procedures should be in place to control the scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting of tapes, and maintaining computer equipment. *Our audit did not identify any significant weakness in the operations procedures of the computer center during our audit.*

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, ECU's operations would be interrupted. To reduce this risk, computer service centers develop business continuity plans. Business continuity procedures should be tested periodically to ensure the recoverability of the data center. *Our audit did not identify any significant weakness in disaster.*