APPROVED BY COMMITTEE 6/8/17

OLD DOMINION UNIVERSITY
BOARD OF VISITORS

AUDIT COMMITTEE
Thursday, April 27, 2017

MINUTES

The Audit Committee of the Board of Visitors met on Thursday, April 27, 2017 at 8:08 a.m. in Committee Room A (Room 2203) of Broderick Dining Commons on the Norfolk campus. Present from the Committee were:

Frank Reidy, Vice Chair
Carlton Bennett, *(ex-officio)*
Mary E. Maniscalco-Theberge '78

Other Board of Visitors members present were:

None

Absent were:

Fred Whyte, Chair
Donna Scassera
Lisa Smith, *(ex-officio)*
Robert M. Tata '86

Also present were:

President John R. Broderick
Velvet L. Grant
David F. Harnage
Casey Kohler
Amanda G. Skaggs
James D. Wright

Mr. Reidy, Vice Chair, called the meeting to order at 8:08 a.m. Dr. Maniscalco-Theberge moved to approve the minutes from the December 8, 2016 meeting. Mr. Bennett seconded the motion and the minutes were unanimously approved by all members present and voting. *(Bennett, Reidy, Maniscalco-Theberge)*

Next, Amanda Skaggs, Internal Audit Director, gave the Auditor's Report. First, she discussed five audits currently underway by her department.

1) ***SoBran Facility Operations***
The audit staff is wrapping up the audit on SoBran Facility Operations which is a joint

effort between the Office of Research and the Old Dominion University Research Foundation. SoBran manages a portion of the University's laboratory space. The audit is looking at the delineation of responsibilities, revenue and expense processes, fixed asset control, internal and external facility inspections and facility access.

2) ***Frank Batten College of Engineering and Technology***
In the Frank Batten College of Engineering and Technology, the audit is focusing on budget management, small purchase credit cards, building access, centers and institutes, use of restricted funds, asset tracking and travel.

3) ***Confucius Institute***
The audit staff is wrapping up field work for calendar year 2015 transactions in the Confucius Institute. Funds provided by Hanban support Chinese language programs at educational institutions. The funding source has requested that audits of the Confucius Institute be performed regularly.

4) ***Facilities Management***
The audit will review different campus programs for which Facilities Management is responsible. It includes fuel and gas cards and cost recoveries after performing maintenance work for various campus departments. Also under review are contract management by the department, planning and estimating, key distribution and retrieval, budget management including expenses, transfers, PCard purchases and preventative maintenance.

5) ***Accounts Receivable***
The Accounts Receivable audit is an integrated one where a senior auditor is paired with the IT audit manager. The department is in the fieldwork stage of this audit. It will focus on cashiering, student billing and Touchnet, which is the system used in the student billing process.

6) **General Accounting**
The Internal Audit Office is partnering with the Auditor of Public Accounts on this audit now in the fieldwork stage. Under review will be journal entries, bank reconciliations, grant and contract reimbursements and reconciliations, management of fixed assets, leases, reconciliation of the state system called Cardinal, indirect costs, access control, and segregation of duties.

7) ***Banner Document Management System (BDMS)***
The audit staff is working on the preliminary survey phase for this audit. BDMS is a repository of electronic documents that support business processes associated with various departments including the Office of Finance and the division of Student Engagement and Enrollment Services. Under review are the controls of the system related to access, data management and the associated assets that will determine whether

the system is operated and configured in a secure, reliable and compliant manner.

Next, Ms. Skaggs discussed other ongoing activities in the department.

1) *Annual Risk Assessment* – This assessment will determine where high risk areas are so that an audit plan can be drafted for the upcoming year.
2) *Consulting Engagements* – The office is currently involved in two engagements.
3) *Investigations/Special Projects* – The office must investigate tips that are received from the Fraud, Waste and Abuse Hotline. There are seven investigations that have been initiated this year with four currently underway. Three claims have been closed and deemed unsubstantiated.
4) *Quality Assurance Review* – It is a requirement that every five years the Office of the Internal Auditor must be audited. During this time, the State Inspector General's Office offers the option to coordinate and find other auditors within the state to perform the review. If an office takes advantage of this coordination, the stipulation is that the same office will volunteer to provide this service to other agencies as well. ODU's Internal Audit Office completed this type of external review in 2014 and this year has provided assurance review services to two other agencies within the Commonwealth. This process also involves being onsite for two to three days to review the participating office's audit work and procedures.
5) *College of Auditors of Virginia Conference* – Old Dominion will be hosting this year's two and a half day conference in Virginia Beach that provide CPEs to its attendees.
6) *Recruitment* – Employee James Harris was with the University for 20 years. He officially retired on March 1. The recruitment process is now underway for his replacement.

Finally, Ms. Skaggs provided details on two audit reports.

1: Accounts Payable Vendor Payments

The objective of this audit was to determine whether processes for vendor payments were in compliance with state and University requirements and whether appropriate internal controls were in place. Accounts Payable processed approximately 16,000 invoices that totaled $126 million for the 12 months ending March 31, 2017.

The overall risk rating was moderate. The system of internal controls in effect over Accounts Payable Vendor Payments was adequate.

The audit focused on prompt payment compliance, general payment controls, vendor table maintenance, segregation of duties, debt set off and 1099 processing.

Observation 1: Prompt Payment Reporting
Lease payments and utility payments were being excluded from the University's prompt payment reporting without meeting the criteria for an allowable exclusion.

Prompt payment provisions require state agencies that acquire goods and services, or that conduct business through contractual agreement with nongovernmental and privately owned businesses, to pay by the required payment due date for delivered goods and services. The University must submit a quarterly report to the state that shows the percentage of on-time payments which includes the number of payments and payment amounts based on criteria set forth in the regulations. Higher education institutions are considered to be in compliance if they report that at least 95% of payments are made on time. For the four quarters tested, Old Dominion reported at least a compliance rate of 95%.

The audit found that while lease and utility payments were being paid on time, they were being excluded from the University's prompt payment reporting without meeting the criteria for an allowable exclusion. Mr. Harnage noted that originally, when prompt payment reports started, there were exclusions for lease and utility payments. This has changed over time. If these payments are included in the report, the University's prompt payment improves. Ms. Skaggs stated that quarterly lease payments approximate $2 million and quarterly utility payments approximate $1.5 million. She also noted that there are some exclusions. These include prepaid leases and vendor payments to governmentally-owned utilities. She stated that the department is now adhering to this reporting requirement.

Observation 2: Debt Set-Off Process
The process designed to intercept vendor payments to offset debts owed to state agencies was not consistently working as intended.

The state has a program that is designed to intercept vendor payments when vendors owe debt to state agencies. The University's process includes retrieving data from the state as to which vendors owe debt and matches those vendors with a list of vendors with which the University does business. When there is a match, the vendor record is flagged so that payments are remitted to the state instead of directly to the vendor. Some vendors were not properly flagged as debt set-off eligible which was caused by the sequence of processing files which overwrote the flag for debt set-off processing. It was recommended that Accounts Payable should work with ITS to fix the process and to validate that all payments that are required to be remitted to the state are processed accordingly. The problem was quickly resolved. It was noted that the corrected process should be monitored at a frequency that would allow for those responsible for the process to know that the process is working properly.

Observation 3: Segregation of Duties
The accounts payable manager had full access to the payment cycle to include the ability to make changes to vendor tables, process invoices for payment, and make disbursements.

Proper segregation of duties includes disallowing an individual full access to the entire payment cycle. The accounts payable manager had full access to the payment cycle to include the ability to make changes to the vendor tables, process invoices for payment and make disbursements. While some mitigating controls exist, including the independent review of checks over $10,000, approval by the ordering department, and department reconciliations of Banner accounts, the controls do not mitigate the risk to an acceptable level. It was recommended that the department remove the conflicting roles so that one individual cannot change vendor tables, process invoices, and make disbursements. This issue has been resolved as well.

2: Cognos/Insight (Operational Data Store)
This system is used by numerous areas to analyze and report on the University's financial, student and human resource records. It is the largest repository of sensitive and regulated University records. The primary data source is Banner which is the University's enterprise resource planning system.

The objective of the audit was to assess the effectiveness of the design and operation of internal controls over the system. The overall risk rating was high. The audit conclusion rating was adequate.

The system of internal controls in effect over Cognos was adequate during the period of review with three reportable items. The audit focused on account management, including access to business intelligence reports and the Operational Data Store, associated hardware/software including configuration, maintenance and security controls in effect over connectivity, and processes ensuring data integrity.

Observation 1: Data Transmission Vulnerabilities
The web servers employ encryption of insufficient strength to protect against unauthorized data disclosure during transmission across the public internet.

The system stores and transmits the University's most sensitive and regulated data. The encryption used is of insufficient strength to protect against unauthorized data disclosure during transmission across the public internet. The encryption is known to be weak and is expressly disallowed by the University's own encryption standard. Vulnerability scans of the web server also confirmed this condition. The recommendation is that the risk of disclosure should be mitigated by either requiring a VPN connection when accessed through the public internet or configuring and maintaining the servers to only support encryption meeting standards for highly sensitive and confidential data. The department is working to have a resolution by June.

Mr. Reidy inquired about any past account breaches to the system resulting from this deficiency. Ms. Skaggs stated that she was not aware of any accounts in this system being breached as a result of this issue.

Observation 2: Electronic Access Controls
Additional actions are needed to ensure security is maintained at levels commensurate with highly confidential and regulated data.

Since the login page is directly accessible from the public internet and is the primary logical access control, the strength of its security should be ascertained.

The application has not been assessed for vulnerabilities with a dedicated web application scanner. An important security implementation is to restrict network traffic to only those ports that are used for necessary data services. This is also consistent with the ITS network management standard.

The system's database host firewalls are not configured to block connections to all unused ports. It is recommended that the web application should be periodically scanned with a dedicated web application scanner and/or a verified-trusted authentication mechanism should be implemented for access to the system from outside of the campus network. The host firewalls should be configured to deny access to unused ports. The department is working on these actions.

Observation 3: Account Management and Data Access Procedures
Account management and administrative access control procedures are not documented or implemented on a level commensurate with data sensitivity.

The audit revealed five conditions to support this observation:

1. Access to reports created in test can be granted to any user including those who have not been authorized to access the type of data shared. Those users with authoring capabilities have not been provided guidance for sharing access.

2. Direct access to the database is not consistently approved by the data owner, nor is the access periodically reviewed for continued necessity. The user's access is approved by the budget unit director and the datamart owner. This practice is in significant contrast to the account management practices and annual audits of Banner user access.

3. Sampled project records do not demonstrate that access to the resulting reports is authorized by respective data owners.

4. Documented procedures do not exist for the creation, suspension, disabling and termination of accounts. This is contrary to the ITS account management standard.

Sampled documentation indicated that the process is not consistent with regard to who should initiate the request and approve the access.

5. Accounts remained in an active state beyond the user's separation date. This resulted from a technical issue with the automated process that is trusted to remove access after termination.

   The recommendation is, if technically possible, to prevent report authors from sharing access to reports, or else policies should be established and communicated to authors. Direct access to any table should require explicit approval by respective data owners. Report access granted to users upon completion of projects should be formally approved by respective data owners or the system owner. Account management policies should be documented and user accounts should be reviewed and validated at least annually. Similar to methods in place for Banner, user accounts should be reviewed and validated at least annually by both data owners and budget unit directors. This affords the opportunity to alter user access based on changes to regulatory requirements, university policies, employee role changes and business necessity.

There being no further business, the meeting was adjourned at 8:29 a.m.