

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT COMMITTEE
January 25, 2002**

AUDIT COMMITTEE
(Open Session)

Friday, January 25, 2002
9:00 - 9:30 a.m.
Board Room, The Rotunda

Committee Members:

Elizabeth A. Twohy, Chair Benjamin P.A. Warthen
Timothy B. Robertson John P. Ackerly, III, Ex Officio

AGENDA

	<u>PAGE</u>
• Information Report (Ms. Deily)	
A. Auditor of Public Accounts (APA) Audit and Management Letter (Ms. Deily to introduce Mr. Walter Kucharski; Mr. Kucharski to report)	1
B. University and Health System Response to the APA Audit and Management Letter (Ms. Deily to introduce Ms. Yoke San Reynolds and Mr. Larry L. Fitzgerald; Ms. Reynolds and Mr. Fitzgerald to report)	2
C. Corporate Compliance Agreement (Ms. Deily to introduce Mr. Ralph Traylor; Mr. Traylor to report)	7

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: January 25, 2002

COMMITTEE: Audit

AGENDA ITEM: Information Report

BACKGROUND: Ms. Deily will introduce Mr. Walter Kucharski, Auditor of Public Accounts of the Commonwealth, who will report on the Auditor of Public Accounts Audit and Management letter. The University and the Health System will respond to the Audit and Management letter.

ACTION REQUIRED: None

UNIVERSITY DIVISION

Recommendation: Implement Complete Exit Interview Procedures

The University has not implemented standard procedures for departments to ensure they properly recover all university property and change security access when an employee leaves. The separation procedure provides departments the opportunity to recover University property such as keys, charge cards, and identification cards and to properly cancel the employee's access to all university systems. In order to make sure that all departments consider these issues when an employee leaves, the University should develop and maintain standard procedures for departmental personnel to follow during the exit conference.

Management Response: Management concurs. The University recently approved a new policy entitled "Responsibility of Managers and Other UVA Officials for Access Privileges" during the summer/fall of 2001. The policy clearly defines who is responsible for ensuring privilege-granting departments are notified when employees, contractors and others no longer need the privileges. It also addresses the issue of collecting physical items such as keys. The policy was placed on the University Human Resources website effective October 15, 2001.

Responsible Area: University Human Resources

Estimated Completion Date: April 1, 2002

Recommendation: Card Members and Supervisors Must Review and Reconcile Charge Statements

The University has issued charge cards to over 1,200 staff for purchasing goods and services that totaled over \$11 million in the past fiscal year. While the University has policies and procedures to ensure that all purchases are appropriate and charges are accurate, we found instances where staff were not following the procedures.

Some managers are not reviewing the purchasing logs and supporting receipts to ensure the appropriateness of cardholder purchases. Managers did not review and approve purchase logs and reconciliations in six of the 19 (32%) statements tested.

Some cardholders are not reconciling their monthly card statement to the purchasing log. We found that two of 19 cardholders (11%) did not properly reconcile their purchasing logs to the card statements.

UNIVERSITY DIVISION, continued

Without the statement review and the reconciliations, unauthorized or inappropriate purchases may go undetected. Failure of cardholders and their managers to follow procedures could allow fraudulent charges or incorrect payments.

Management should enforce compliance with procedures over the charge card payment and reconciliation process and should revoke charge cards from cardholders who do not follow policies and procedures. Ensuring employees follow the internal controls over the Small Purchase Charge Card Program will reduce the risk of fraudulent and incorrect charges and ensure purchases are appropriate.

Management Response: Management concurs. In response to the recent findings of State auditors that some Purchasing Card users have not followed specific rules, Procurement Services has revised its training materials, its web site, and the University's Financial and Administrative Policies and Procedures to place greater emphasis on the necessity of strictly adhering to the rules governing the use of the Purchasing Card. Procurement Services has also described more carefully the penalties that will be assessed for the failure to comply with specific rules.

Procurement Services will continue to conduct random checks to verify cardholder and supervisor compliance with Purchasing Card policy and procedure. In addition, the University's Audit Department conducts its own periodic reviews to verify cardholder and supervisor compliance. Procurement Services will immediately suspend or permanently revoke the privileges of any cardholder found not to be in compliance with Purchasing Card policy and procedure.

Responsible Area: Procurement Services
Estimated Completion Date: December 14, 2001

HEALTH SYSTEM DIVISION

Recommendation: Continue Security Initiative Over Critical Information Systems and Network

The Health Systems Computing Services (HSCS) has continued its effort to enhance security over the Health System's information systems. As custodian over data resources that are vital to the Health System's operations, HSCS must implement and maintain strong security controls that adequately safeguard Health System's information resources and protect the privacy of its patients. Federal regulations, in the form of the Health Insurance Portability and Accountability Act (HIPAA), and other recent events have heightened awareness of the need for strong information security and contingency plans.

To increase security within the entire information system environment, Health System's management developed a comprehensive security strategy. The plan has a two-phase implementation. In Phase One, management hired a data security consulting firm to perform a Risk Analysis and Vulnerability Assessment. The assessment, completed in May 2000, addressed several vulnerabilities in the Health System's clinical subnet security system, including a lack of centralized security management, insufficient network controls, inadequate data security policies, and improper configurations of hardware. Although the Health System operates a subnet of the University's network, regulatory requirements and oversight are much more stringent due to Protected Health Information.

The Health System's management has begun Phase Two, the Remediation Phase. After correcting the most vulnerable network concerns, management hired another data security consultant to assist in developing a comprehensive information security program. The plan includes firewall security, which protects the entire Health System network, data encryption and token card one-time password generation for all data communication originating outside the Health System clinical subnet, and network monitoring equipment and software to detect and block attempts of unauthorized or inappropriate clinical subnet access.

HEALTH SYSTEM DIVISION, continued

HSCS management has established a clinical subnet architecture plan and is awaiting delivery of equipment. After installing the equipment, HSCS management will begin converting its user's network access to the new system. HSCS has also hired a new director whose duties will include managing data security. Finally, the Health System is working with Information Technology and Communications (ITC) at the University to develop comprehensive information security policies. Health System management should continue with the development and implementation of the comprehensive information security program.

Management Response: Management concurs. Management is aware of the additional requirements placed on the Health System's portion of the UVA Network due to protected health information with the April 2003 HIPAA compliance date. The Health Systems clinical subnetwork design is completed and equipment has been ordered. The equipment is in the process of being received. By March 31, 2002, new equipment required to secure the clinical subnetwork will be installed. By June 30, 2002, migration will begin for approximately 4,000 Health System end user devices to move on to the secured clinical subnetwork, thereby bringing the Health System toward compliance with HIPAA and JCAHO information management requirements.

Responsible Area: Health Systems Computing Services
Estimated Completion Date: April 14, 2003

Recommendation: Implement the New Change Control Procedures Over PeopleSoft and Oracle Applications

In our previous audit, we recommended that management of the Health System's Administrative Services Division (Administrative Services) develop and implement formal change control procedures to manage changes and upgrades to its PeopleSoft and Oracle software applications. During the year, Administrative Services developed a procedure entitled "Change Control Policy and Procedures for PeopleSoft/Oracle Applications"; however, management has only recently begun to implement these procedures.

We recommend that Administrative Services continue implementing the new procedures. Management should ensure that the change management procedures include logging and tracking all changes

HEALTH SYSTEM DIVISION, continued

throughout the program change process and provide a record of all changes made. These procedures will document the data owner and management's approval of changes and provide a complete program change record for use in system upgrades.

Management Response: Management concurs. The recommendations have been fully implemented as of September 1, 2001.

PeopleSoft operates under the Administrative Services division of the Health System. Change control procedures were created and documented by the PeopleSoft team over the last several months. As of September 1, 2001, procedures became operational. These procedures assure change to production systems occur only after the following steps: 1) Sign off by technical support staff who completed successful unit testing, 2) Documentation of system customization for purposes of efficient system upgrades, and 3) Audit trail or PeopleSoft Change Control log, which tracks service requests and current status/completion. PeopleSoft operations and support has begun migration to a reporting structure through HSCS. This organizational change is expected to be fully completed by December 1, 2001.

Responsible Area: Health System Computing Services
Estimated Completion Date: December 1, 2001

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: January 25, 2002

COMMITTEE: Audit

AGENDA ITEM: Information Report

BACKGROUND: Ms. Deily will introduce Mr. Ralph Traylor, who will give an update on the Corporate Compliance Agreement.

ACTION REQUIRED: None