Audit Report

University System of Maryland
Salisbury University

June 2009

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.
- Electronic copies of our audit reports can be viewed or downloaded from our website at http://www.ola.state.md.us.
- Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.
- The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Bruce A. Myers, CPA
Legislative Auditor

June 22, 2009

Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Senator Verna L. Jones, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the University System of Maryland (USM) – Salisbury University (SU) for the period beginning October 1, 2005 and ending August 27, 2008. SU is a comprehensive public institution of the University System of Maryland and provides a broad range of baccalaureate programs as well as selected professionally-oriented master's programs.

Our audit disclosed that several individuals had improper access to critical data and transactions on SU's automated systems, including student residency status and disbursement transactions. In addition, SU's internal computer network was not sufficiently secured from both internal and external exposures, and controls over critical systems and databases were inadequate.

Our audit also disclosed that SU had not established sufficient control over voided transactions recorded on its cash register system. Finally, we noted internal control and record keeping deficiencies over SU's dining services materials and supplies, and equipment.

An Executive Summary of our findings can be found on page 5. The USM Office response to this audit, on behalf of SU, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by SU.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

*** Denotes item repeated in full or part from preceding audit report**

Executive Summary

Legislative Audit Report on University System of Maryland
Salisbury University (SU)
June 2009

- **SU did not adequately restrict access to critical data on its systems, including student residency status and disbursement transactions.**

  SU should establish the recommended procedures and controls to ensure that all critical information recorded in its computer system is authorized and accurate.

- **SU's internal computer network was not adequately secured from both internal and external exposures. For example, firewalls were not adequately configured. In addition, controls over critical systems and databases were inadequate.**

  SU should take the recommended corrective actions to help prevent and detect unauthorized access and the processing of unauthorized transactions.

- **Cashiers voided transactions on the automated cash register system without independent approval, and there was no documentation to substantiate that these transactions were subsequently reviewed by supervisory personnel.**

  SU should remove the ability of cashiers to void transactions and ensure that documentation of supervisory review and approval of voided transactions is maintained.

- **Internal control and recordkeeping deficiencies were noted over materials and supplies for dining services and certain equipment.**

  SU should take the recommended actions to improve controls in these areas.

Background Information

Agency Responsibilities

Salisbury University (SU) is a comprehensive public institution of the University System of Maryland and operates under the jurisdiction of the System's Board of Regents. SU provides a broad range of baccalaureate programs as well as selected professionally-oriented master's programs. Student enrollment for the Fall 2008 semester totaled 7,868, including 7,281 undergraduate students and 587 graduate students. SU's budget is funded by unrestricted revenues, such as tuition and fees and a State general fund appropriation, and restricted revenues, such as federal grants and contracts. According to the State's accounting records, SU's revenues for fiscal year 2008 totaled approximately $129 million, which included a State general fund appropriation of approximately $35 million.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the 10 findings contained in our preceding audit report dated March 17, 2006. We determined that SU satisfactorily addressed 7 of the findings. The 3 remaining findings are repeated, and appear as 2 items, in this report.

Findings and Recommendations

Information Systems Security and Control

Background

Salisbury University (SU) maintains a campus-wide network that supports both administrative and academic operations. The network includes Internet connectivity, various administrative servers, and firewalls. SU's Information Technology Department (ITD) maintains critical application systems supporting Student Administration, Human Resources, and Financial Information Systems. ITD also manages the development, maintenance, and support of the University's information technology infrastructure including networking, telecommunications, and business information systems.

Finding 1
SU did not adequately control certain critical transactions processed on its automated system.

Analysis

SU did not adequately control certain critical transactions on its automated systems to ensure that only authorized transactions were processed. Specifically, we noted the following conditions:

- SU generated output reports of changes to student residency status that were subject to supervisory review and approval. However, the SU employee who reviewed the output reports also had the capability to change student residency status without independent authorization. Student residency status is a critical data element because of the significant differences between in-state and out-of-state tuition rates. For example, tuition and fees for Maryland residents was $3,246 for the Fall 2008 semester, whereas tuition and fees for out-of-state students was $7,397. A similar condition was commented upon in our preceding audit report.

- Four information technology employees had the ability to initiate and approve purchase orders, receive goods, enter invoices, and add vendors even though their job duties did not require such access. Although we noted that no such transactions were processed by these four employees during our audit period, these employees could potentially process unauthorized purchasing and disbursement transactions without detection. According to its records, SU processed expenditures (excluding payroll) totaling approximately $47.7 million during fiscal year 2008.

As a result of these deficiencies, unauthorized transactions could be processed without detection.

Recommendation 1
We recommend that SU

a. ensure that output reports of student residency changes on its automated system are reviewed by independent supervisory personnel (repeat),
b. use available security features by establishing independent online approval requirements for all critical purchasing and disbursement transactions, and
c. restrict access to critical transactions to only those employees whose job responsibilities require such access.

Finding 2
Key administrative systems on the computer network were not adequately secured.

Analysis
Key administrative systems (for example, the Financial and Student Administration Systems) were not adequately protected from both internal and external exposures. Specifically, we noted the following conditions:

- Numerous widely accessible servers were located on the internal network rather than in a separate network zone to minimize security risks. These widely accessible servers, which could potentially be compromised, exposed the internal network to attack from external sources.

- Firewall rules were not configured to adequately secure connections into the network from the Internet and from untrusted portions of the University's network (for example, student computer labs). Therefore, critical network devices, critical systems, and administrative workstations were susceptible to attacks, which could result in a loss of data integrity, the destruction of critical files, or the interruption of critical network services.

Similar conditions were commented upon in our preceding audit report.

Recommendation 2
We recommend

a. that SU place all widely accessible servers in a separate network zone to minimize security risks (repeat), and

b. that SU configure its firewalls to adequately secure its network using a "Least Privilege" security strategy giving individuals only the access necessary to perform assigned tasks (repeat).

Finding 3
Controls over the Student Administration, Human Resources, and Financial Information Systems were not adequate to help prevent and detect unauthorized and inappropriate access.

Analysis
We noted the following account and monitoring control deficiencies regarding the Student Administration, Human Resources, and Financial Information Systems:

- As of December 10, 2008, there were 49 active accounts on the Student Administration and Human Resources critical application systems that belonged to terminated employees. According to SU's records, these accounts had been active for a range of 19 to 344 days after the effective termination date of the respective employees. USM *Guidelines in Response to the State's IT Security Policy* Version 1.5, dated March 2008, stipulate that Institutions must implement and document processes to ensure that access rights reflect employee status, including changes in employee status. The *Guidelines* further stipulate that, for critical systems, employees' access rights should be modified, as appropriate, by the close of business on the same day.

- Critical security events (for example, adding or removing a login account) and audit events were not logged for the Student Administration, Human Resources, and Financial Information Systems' databases. Accordingly, significant database security violations could go undetected, thus permitting unauthorized or inappropriate activities to adversely affect the integrity of the production data files. USM *Guidelines in Response to the State's IT Security Policy* stipulate that Institutions must ensure that all critical systems have the ability to log and report specific security incidents and all attempted violations of system security. In addition, institutions must establish and document processes for reviewing IT security violations on a daily basis**.**

Recommendation 3

We recommend that, in accordance with USM *Guidelines*, SU

a. ensure that, for all critical systems, employee access rights are modified, as appropriate, by the close of business on the same day as the change in employee status occurs;

b. log all significant security and audit events for its critical databases; and

c. review these logs on a daily basis, perform investigations where necessary, document the reviews and investigations, and retain them for future verification.

Cash Receipts

Finding 4

Employees who received collections processed voided transactions without independent approval, and there was no documentation of a subsequent supervisory review.

Analysis

Cashier's Office employees who received collections and recorded them on the automated cash register system also processed voided transactions on the system without independent approval. Although we were advised by SU management that supervisory personnel reviewed voided transactions at the close of each business day, such reviews were not documented. As a result of these conditions, collections could be misappropriated without detection. According to SU's records, during fiscal year 2008, collections received by the Cashier's Office and related voided transactions totaled approximately $39.4 million and $519,000, respectively.

Recommendation 4

We recommend

a. that cashiers not have the ability to void transactions on the automated cash register system, and

b. that documentation of the supervisory review and approval of voided transactions be maintained.

Materials and Supplies

Finding 5
Materials and supplies for SU's dining services were not adequately controlled.

Analysis
Internal control and record keeping deficiencies were noted over SU's dining services materials and supplies. According to SU's records, during fiscal year 2008, expenditures for these materials and supplies totaled approximately $3.5 million. Specifically, we noted the following conditions:

- Access to the dining services storerooms was not properly restricted. In this regard, the storerooms remained open during the day and were only locked overnight. SU management personnel advised us that 14 employees had unrestricted access to the storerooms.

- Perpetual inventory records were not maintained. Additionally, requisition forms were not used to withdraw items from the inventory; rather, the items were removed from the storerooms by any of the dietary staff when needed. Furthermore, although physical inventories were conducted weekly, the physical counts served only to determine quantities of items that needed to be reordered.

As a result of these deficiencies, SU's management may not readily detect irregularities related to these inventories. The USM *Policy for Capitalization and Inventory Control* requires institutions to maintain an inventory system appropriate to the value of the items held for resale. The *Policy* also requires the applicable institution to take a physical inventory of these items at year-end.

Recommendation 5
We recommend that SU comply with the aforementioned requirements of the USM *Policy for Capitalization and Inventory Control*. In addition, we recommend that SU
a. control access to the dining services storerooms; and
b. at least annually, reconcile the physical inventory of the materials and supplies for dining room services with the perpetual inventory records.

Equipment

Finding 6
Acquisitions were not always recorded in the equipment records and equipment was not always tagged for identification and control purposes.

Analysis
Equipment acquired for SU's Teacher Education and Technology Complex (TETC) was not always recorded in the detail records, and equipment was not always tagged for identification and control purposes. Specifically, our test of 30 capital equipment items purchased prior to June 30, 2008 for the TETC building, totaling approximately $137,500, disclosed that 26 items totaling approximately $126,500 were not posted to the detail equipment records as of November 25, 2008, as required by the USM *Policy for Capitalization and Inventory Control*. Additionally, 3 of the 30 items totaling approximately $5,800 were not tagged for identification and control purposes. Subsequent to our audit, we were advised that all of the equipment acquired for the TETC building had been recorded in the detail records and the book value of the acquired equipment totaled approximately $5 million as of March 2009.

Recommendation 6
We recommend that SU

a. record equipment acquisitions in the detail records, as required by the USM *Policy for Capitalization and Inventory Control*; and
b. properly tag its equipment items for identification and control purposes.

Audit Scope, Objectives, and Methodology

We have audited the University System of Maryland (USM) – Salisbury University (SU) for the period beginning October 1, 2005 and ending August 27, 2008. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine SU's financial transactions, records and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations. We also determined the status of the findings contained in our preceding audit report.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of materiality and risk. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of SU's operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

Our audit did not include certain support services provided to SU by the USM Office. These support services (for example, endowment accounting and bond financing) are included within the scope of our audit of the USM Office. In addition, our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of SU's compliance with federal laws and regulations pertaining to those programs because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including the components of the USM.

SU's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect SU's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to SU that did not warrant inclusion in this report.

The USM Office response, on behalf of SU, to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the USM Office regarding the results of our review of its response.

APPENDIX

OFFICE OF THE CHANCELLOR

June 17, 2009

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, Maryland 21201

Re: Audit of University System of Maryland – Salisbury University
Period of Audit: October 1, 2005 – August 27, 2008

Dear Mr. Myers:

I have enclosed the University System of Maryland – Salisbury University's response to your draft report covering the examination of the accounts and records of Salisbury University for the period beginning October 1, 2005 and ending August 27, 2008. Our comments refer to the individual items contained in the report.

Sincerely,

WE Kirwan

William E. Kirwan
Chancellor

Enclosure

WEK:mpk

cc: Dr. Janet Dudley-Esbach, President, Salisbury University
Mr. Clifford Kendall, Chair, Board of Regents
Mr. Robert L. Page, Comptroller, USM
Mr. Kevin M. O'Keefe, Chair, MHEC
Dr. James E. Lyons, Sr., Secretary of Higher Education, MHEC
Mr. Dave Mosca, Director of Internal Audit, USM

1807 University of Maryland, Baltimore
1856 University of Maryland, College Park
1865 Bowie State University
1866 Towson University
1886 University of Maryland Eastern Shore
1898 Frostburg State University
1900 Coppin State University
1925 Salisbury University
1925 University of Baltimore
1925 University of Maryland Center for Environmental Science
1947 University of Maryland University College
1966 University of Maryland, Baltimore County
1985 University of Maryland Biotechnology Institute

Findings and Recommendations

Information Systems Security and Control

Finding 1
SU did not adequately control certain critical transactions processed on its automated system.

Recommendation 1
We recommend that SU

a. ensure that output reports of student residency changes on its automated system are reviewed by independent supervisory personnel (repeat),
b. use available security features by establishing independent online approval requirements for all critical purchasing and disbursement transactions, and
c. restrict access to critical transactions to only those employees whose job responsibilities require such access.

Response 1
The University does not agree with the finding. While it is true that the supervisory employee who reviews the report has the capability to change a residency status, this supervisory employee has not made a residency change since January 2007 and, of the 49 total changes made by said employee during the audit period, 48 involved changes from an "in-state" to an "out-of-state" residency status. The one change to "in-state" was reviewed for propriety by an independent employee. Consequently, we respectfully maintain that employees independent of the residency change are reviewing change propriety and documenting the review in accordance with prior audit recommendations. However, to provide further assurance that residency changes are reviewed by independent personnel, we created a new report on May 5, 2009 that identifies all residency status changes made by the aforementioned supervisory employee. This new report will be generated monthly and is only accessible by one employee. When status changes appear on the report, that employee will continue to review the changes made by the supervisory employee.

The University uses the PeopleSoft system to establish independent online approval paths, but no such option exists for residency status changes. The independent approval paths for purchasing and disbursement do exist but those four information technology employees had access to the approval paths as well.

The access to the four information technology employees was removed on April 1, 2009. We believe this access was a remnant of the PeopleSoft implementation

almost five years ago. It is very important to note that queries of the system indicated that these four employees have never created purchasing or disbursement transactions (e.g., purchase orders, receipts, vouchers or vendors). However, even if these four employees did create an authorized transaction, they could not have actually effected a vendor payment as other controls are in place that would have prevented or detected such transactions. We are ready to demonstrate these compensating controls.[1]

Finding 2
Key administrative systems on the computer network were not adequately secured.

Recommendation 2
We recommend

a. that SU place all widely accessible servers in a separate network zone to minimize security risks (repeat), and

b. that SU configure its firewalls to adequately secure its network using a "Least Privilege" security strategy giving individuals only the access necessary to perform assigned tasks (repeat).

Response 2
The University agrees with the network finding, but we want to reiterate the amount of time and money that was expended to address prior audit network architecture findings. We believed we had adequately segregated the network. Nevertheless, we will relocate the widely accessible servers in several separate DMZ networks to provide the additional isolation by August 31, 2009.

The University agrees with the firewall rules finding. A variety of firewall rules issues were fixed during January 2009 through March 2009 using a "Least Privilege" security strategy. Other firewall issues will be resolved by October 31, 2009.

[1] **Auditor's Comment**: The University's response indicates disagreement with the finding and analysis of this issue. However, its response also specifies the actions that will be taken which, if implemented, should fully address the audit recommendations.

Finding 3
Controls over the Student Administration, Human Resources, and Financial Information Systems were not adequate to help prevent and detect unauthorized and inappropriate access.

Recommendation 3
We recommend that, in accordance with USM *Guidelines*, SU

a. ensure that, for all critical systems, employee access rights are modified, as appropriate, by the close of business on the same day as the change in employee status occurs;
b. log all significant security and audit events for its critical databases; and
c. review these logs on a daily basis, perform investigations where necessary, document the reviews and investigations, and retain them for future verification.

Response 3
The University agrees with the access finding. The accounts in question belonged to certain employee categories. By October 31, 2009, we will develop an automated means to create and delete account access on a daily basis according to employment status.

The University agrees with the logging finding. During March 2009, we reconfigured the monitoring software and began logging the critical database security and audit events. We are reviewing the logs daily and investigating events when appropriate. We are retaining the logs for future verification.

Cash Receipts

Finding 4
Employees who received collections processed voided transactions without independent approval, and there was no documentation of a subsequent supervisory review.

Recommendation 4
We recommend

a. that cashiers not have the ability to void transactions on the automated cash register system, and
b. that documentation of the supervisory review and approval of voided transactions be maintained.

Response 4

The University does not agree with the finding. The Cashier's Office supervisor reviews voids for propriety as part of the verification the supervisor performs on each cashier's daily settlement. The supervisor documents the verification on the settlement sheet, and since voids are part of the settlement, by extension we contend that we are documenting our verification of void propriety. However during March 2009, the supervisor began documenting the review directly on the voided receipt itself. Furthermore, on April 28, 2009 void receipt functionality was removed from Cashier's Office employees and provided to two employees who do not have access to process cash receipts.[2]

Materials and Supplies

Finding 5
Materials and supplies for SU's dining services were not adequately controlled.

Recommendation 5
We recommend that SU comply with the aforementioned requirements of the USM *Policy for Capitalization and Inventory Control*. In addition, we, recommend that SU

a. control access to the dining services storerooms; and
b. at least annually, reconcile the physical inventory of the materials and supplies for dining room services with the perpetual inventory records.

Response 5
The University agrees with the storeroom access finding and access has been restricted. Doors to both storerooms are now locked throughout the day with access restricted to 13 storeroom and management employees. Camera coverage of strategic entrances and exits continues to exist.

The University partially agrees with the perpetual inventory finding. As noted above, the USM *Policy for Capitalization and Inventory Control* does require institutions to maintain an inventory system appropriate to the value of the items held for resale and it does require that a physical inventory of these items be taken at year-end. What isn't addressed above is that the USM policy also indicates that the institution is to determine the appropriate inventory system. In the spirit of

[2] **Auditor's Comment**: The University's response indicates disagreement with the finding and analysis of this issue. However, its response also specifies the actions that will be taken which, if implemented, should fully address the audit recommendations.

cooperation, we will implement, by August 1, 2009, a perpetual inventory system that uses requisitioning to record inventory withdrawals. At the University's discretion, we may limit the requisitioning process to only include material dollar amounts and/or sensitive items. On a fiscal year basis, requisitions will be used on at least 90% of Dining Services' food and non-food resale inventory expenses. On an annual basis at least, we will reconcile the actual inventory counts to the perpetual inventory records.[3]

Equipment

Finding 6
Acquisitions were not always recorded in the equipment records and equipment was not always tagged for identification and control purposes.

Recommendation 6
We recommend that SU

a. record equipment acquisitions in the detail records, as required by the USM *Policy for Capitalization and Inventory Control*; and
b. properly tag its equipment items for identification and control purposes.

Response 6
The University agrees with the findings. By February 28, 2009, all of the TETC equipment had been identified, tagged and recorded in the inventory system. The above findings were related to equipment purchased by the TETC general contractor using capital appropriations and were caused by communication and coordination issues. The issues are atypical of our usual equipment recordation and tagging proficiency. By September 1, 2009, the University will implement procedures to be used in all future capital projects to ensure that equipment is recorded and tagged timely.

[3] **Auditor's Comment**: The University's response indicates that it only partially agrees with the finding and analysis of this issue. However, its response also specifies the actions that will be taken which, if implemented, should fully address the audit recommendations.

AUDIT TEAM

Mark A. Ermer, CPA
Audit Manager

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

Ken H. Johanning, CFE
Senior Auditor

R. Brendan Coffey, CPA
Edwin L. Paul, CPA
David J. Burger
Information Systems Senior Auditors

R. Frank Abel, CPA, CFE
Joseph E. McWilliams
Staff Auditors

Michael K. Bliss
Information Systems Staff Auditor