Audit Report

St. Mary's College of Maryland

November 2013

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

November 19, 2013

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Delegate Guy J. Guzzone, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited St. Mary's College of Maryland (the College) for the period beginning April 13, 2009 and ending June 30, 2012. The College is a public, liberal arts honors college that offers undergraduate and graduate degree programs in various disciplines. The College is governed by a Board of Trustees as authorized by the Education Article, Title 14, Subtitle 4 of the Annotated Code of Maryland.

Our audit disclosed that the College did not establish proper controls over certain information technology functions, such as the granting of user access capabilities and the monitoring of computer security. For example, certain employees were assigned incompatible or unnecessary capabilities affecting student information and financial system records. Also, security event logging was not enabled for certain computer servers and the College lacked assurance that malware protection software had been installed on all computers. Finally, the College did not document the performance of procedures designed to verify cash receipt deposits and did not sufficiently ensure the propriety of invoices from its food service contractor.

An executive summary of our findings can be found on page 5. The response from the College to our findings and recommendations is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by the College.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

Table of Contents

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

Executive Summary

Legislative Audit Report on St. Mary's College of Maryland
November 2013

- **The College lacked effective internal controls over critical online purchases and disbursements, and employee access to certain critical functions was not properly restricted (Finding 1).**

  The College should use the available security features of its student information and financial system and sufficiently restrict user access to eliminate incompatible duties and unnecessary access over critical functions such as purchasing and disbursement processing.

- **The College lacked sufficient controls over critical components of its student information and financial system to protect against data security and operational risks (Findings 2–5).**

  The College should implement appropriate access and monitoring controls over critical components of its student information and financial system and take other recommended corrective actions.

- **The College lacked controls to ensure the propriety of student refunds and non-cash credits (Finding 6).**

  The College should ensure that refunds and non-cash credits recorded in the College's student records are reviewed and approved by independent supervisory personnel.

- **The College did not maintain documentation to substantiate that collections were verified to the deposit documents (Finding 7).**

  The College should document the verification of collections to deposit.

- **The College did not sufficiently verify the billings of its food service contractor (Finding 8).**

  The College should obtain appropriate support and verify the propriety of billed costs prior to processing payments to its food service contractor.

Background Information

Agency Responsibilities

St. Mary's College of Maryland is a public, liberal arts honors college that offers undergraduate degree programs in various disciplines and a graduate degree in Masters of Arts in Teaching. The College is governed by a Board of Trustees as authorized by the Education Article, Title 14, Subtitle 4 of the Annotated Code of Maryland. This law provides the Board with broad authority in managing the affairs of the College and specifies that the Board may not be superseded in its authority by any State agency or office except as expressly provided for in law. Furthermore, the law provides for the College to receive State general funds in the form of an annual grant. According to the College's records, fiscal year 2012 revenues totaled approximately $67.5 million, which included a State general fund appropriation of approximately $18 million, and student enrollment for the spring 2012 semester totaled 1,939.

Status of Findings From Preceding Audit Report

We reviewed the status of the 15 findings included in our preceding audit report dated February 16, 2010. We determined that the College satisfactorily addressed 14 of these findings. The remaining finding is repeated in this report.

Findings and Recommendations

Information Systems Security and Control

Background

The College's Office of Information Technology provides information systems support to the College through the operation and maintenance of campus-wide administrative applications, such as the student information and financial system. The Office also operates an integrated administrative and academic computer network that provides connections to a substantial number of servers used for administrative applications and related databases. The campus network also includes separate file servers, Internet connectivity, and firewalls.

Finding 1
The College did not establish independent online approval of certain critical transactions and did not ensure that user access capabilities were properly restricted.

Analysis

The College did not properly use the security features of its student information and financial system to establish proper controls over transaction processing and to restrict user access capabilities. Our review of critical online purchase and disbursement functions disclosed that eight employees had the capability to create purchase orders for amounts up to $10,000 without obtaining independent approval and with the ability to bypass the requisition process. Furthermore, these eight employees could add or modify vendors in the system. Additionally, four of these employees had the capability to process and approve the related vendor invoices for payment. Consequently, unauthorized purchases could be made and not readily detected by the College's management. According to the State's accounting records, the College processed disbursements totaling approximately $30 million during fiscal year 2012.

In addition, although the College annually reviewed system reports of the access capabilities assigned to its employees, at the time of our review, a number of employees had been assigned capabilities that were not needed to perform their duties.

Access to Critical Automated System Functions		
Critical Student and Financial System Function	**Number of Employees With Access[1]**	**Number of Employees With Unnecessary Access**
Modify Purchase/Disbursement Transactions	19	16
Change Student Residency Status	10	8
Modify Student Account Data (tuition and fees)	16	7
Modify Student Accounts (issue non-cash credits)	6	4
Modify Refunds Issued	5	3
Change Student Information (name and address)	29	3
Change Student Grades	10	7

[1]Employees may be assigned access to multiple critical functions.

A similar comment on unnecessary access was included in our preceding audit report.

According to industry best practices, as described by the Department of Information Technology's *State Information Technology Access Control Standard*, system access should be limited to the appropriate authorized individuals and be properly controlled.

Recommendation 1

We recommend that the College

a. use the available security features of its automated system to require independent approval for critical transactions; and

b. assign user access capabilities to only those employees who require such capabilities to perform their assigned job duties, and immediately remove the aforementioned unnecessary access capabilities (repeat).

We advised the College on accomplishing the necessary separation of duties using existing personnel.

Finding 2
Certain security events were not being logged and monitored and certain individuals could make unauthorized changes to critical programs without detection.

Analysis
Access and monitoring controls over critical components of the student information and financial system were not adequate to detect or prevent unauthorized access and changes. Specifically, we noted the following conditions:

- Six accounts with database administrator privileges were not set to log modifications to student information and financial system database tables. In addition, 25 critical database tables were not set to log direct modifications. Finally, reviews of database logs were not independent since the reviews were performed by a database administrator and all database administrators could also make changes to the database.

- Controls over security event monitoring of the server hosting the student information and financial system database and application were deficient because the audit service (which logged critical server security events) was not set to begin when the server was restarted. As a result, a shutdown of this server would disable all logging until manually re-enabled by a network administrator. In addition, we were advised that reviews were not performed of the audit logs that were generated.

- Twenty-six accounts used by seven individuals had unnecessary direct modification access to the student information and financial system's production programs. As a result of this access, unauthorized changes could be made to these programs.

Best practices as noted in the University System of Maryland (USM) *Guidelines in Response to the State's IT Security Policy* require institutions to maintain appropriate audit trails of events and actions related to critical applications and data and further require that these actions be independently reviewed and documented.

Recommendation 2
We recommend that the College implement appropriate access and monitoring controls over critical components of its student information and financial system. In this regard, we made detailed recommendations to the College which, if implemented, would ensure that security events are logged and reviewed, and unnecessary access is eliminated.

Finding 3
The College's contract with a cloud service provider did not properly protect the College against certain security and operational risks.

Analysis

The College's contract with a cloud service provider did not properly protect the College against certain security and operational risks, including the potential exposure of sensitive information such as students' social security numbers and other personal information. For example, we noted the following contract deficiencies:

- The contract did not require the service provider to submit to a third-party review which would provide the College assurance as to the security and confidentiality of its data.

- The contract did not contain a clause or provision providing for the secure disposal and complete removal of the College data from all storage media upon termination of services.

- The contract did not define security incidents and the actions to be initiated by both parties in the event that such incidents were to occur.

Without contractual language that addresses the above-mentioned factors, the College lacked assurance that adequate security controls existed over its data. In addition, the contract included a disclaimer of liability relating to service quality and all warranties, implicit or explicit. Consequently, the College's remedies for recovery against the contractor, in the event of problems, were limited or did not exist. We were advised that the contract, which provided for data backup storage, has since been terminated. The Cloud Security Alliance's best practices in cloud computing include detailing the specific factors mentioned above, including establishing liability expectations, in clear and concise contractual language, to limit operational and security risks.

Recommendation 3

We recommend that, when contracting with a cloud service provider, the College ensure that the related contract addresses significant data security and operational risks, including the aforementioned risks.

Finding 4
The College lacked assurance that all of its active computers were properly protected from malware.

Analysis
The College's malware protection program for its network of workstations and servers was insufficient. For example, the College lacked assurance that malware protection software was installed on all of the College's workstations and servers. As of October 2012, the College's malware protection tool reported that the Campus network included approximately 1,200 computers that did not have malware protection software installed. We were advised that this information was unreliable because it included numerous retired workstations and servers that had not been removed from the College's network directory of computers. As a result, the College did not know the number or identity of computers that did not have malware protection software installed. However, our review of the malware protection software management tool's list of servers that did not have malware protection software installed disclosed at least 10 active servers, including critical student information web and database servers, without the malware protection software installed.

Best practices, as noted in the *USM Guidelines in Response to the State IT Security Policy*, state that standard virus protection programs must be installed, updated, and maintained on all microcomputers, LAN servers, and mail servers.

Recommendation 4
We recommend that the College ensure that malware protection software is installed on all of the College's computers that require such software.

Finding 5
Backup procedures for certain critical servers and network devices did not provide adequate safeguards in the event of a disaster.

Analysis
Backup configurations for certain devices and servers either did not exist or were not stored at an offsite location. Specifically, we noted the following conditions:

- Backup configuration files for two network monitoring devices and a related management server did not exist. In the event of a disaster affecting these devices, their configurations could be lost, resulting in significant delays (of an undetermined period of time) in restoring network capabilities, above and

beyond the expected delays that would exist if secure offsite backups of these devices were readily available.

- Backup configurations for certain critical servers supporting the College's student information and financial applications and the College's primary firewalls were not stored at an appropriate offsite location. Instead, these backups were stored at an on-campus location in close proximity to the College data center. In the event of a localized disaster affecting both the data center and the backup facility, data could be lost which could not be readily recreated.

According to the State of Maryland *Disaster Recovery Guidelines*, backup media should be created and stored offsite in a secure, environmentally controlled location.

Recommendation 5
We recommend that the College perform periodic backups of all critical servers and network devices and store these backups offsite in a secure environmentally controlled location.

Student Accounts Receivable

Finding 6
The College lacked controls to ensure the propriety of refund and non-cash credit transactions.

Analysis
Controls had not been established to ensure the propriety of refund and non-cash credit transactions related to student accounts receivable. Specifically, the supervisory employee responsible for approving student refunds and non-cash credit adjustments also had the capability to initiate the same transactions in the College's student information and financial system. Furthermore, although the College required independent, dual signatures on resultant refund checks, we were advised by two individuals responsible for the second signature that they relied on the aforementioned employee to determine the refund's propriety.

As a result of these control deficiencies, assurance was lacking that critical transactions recorded in the College's system related to student accounts receivable were proper. During fiscal year 2012, according to the College's records, student refunds and non-cash credit adjustments totaled $818,281 and $37,266, respectively.

Recommendation 6
We recommend that

a. **adequate separation of duties be established so that employees who approve student refunds cannot initiate non-cash credit transactions, and**
b. **individuals approving the refund checks perform a documented review of the appropriate supporting documentation.**

We advised the College on accomplishing the necessary separation of duties using existing personnel.

Cash Receipts

Finding 7
Deposit verifications were not documented.

Analysis
Although the College advised us that collections received by the Finance Office were independently compared to deposit documents, evidence that this procedure was performed was lacking. This condition resulted in a lack of assurance that all collections were deposited. According to State accounting records, the College's cash receipts received by the Finance Office totaled approximately $24.7 million in fiscal year 2012. The Comptroller of Maryland's *Accounting Procedures Manual* requires that receipts recorded on initial source documents be traced to deposit by an employee independent of the cash receipts process. The *Manual* also states that critical control procedures should be documented.

Recommendation 7
We recommend that the College maintain documentation to substantiate that collections were verified to the related deposit documents (for example, validated bank deposit records).

Contractual Services

Finding 8
The College did not sufficiently verify the billings of its food service contractor.

Analysis
The College did not ensure the accuracy of certain invoiced charges of its food service contractor. Although the College received and reviewed certain financial

reports included with each weekly invoice, support for vendor payroll costs was not routinely obtained by the College. Specifically, time summaries for the billed labor portion of the invoice were only requested from the contractor for two invoices each year. Furthermore, for the two calendar year 2011 invoices totaling $228,890 for which time summaries were received, there was no evidence that the College verified that these summaries supported the billed costs.

Effective August 5, 2005, the College contracted with its current food service contractor on a cost-plus fee basis for a five-year period and extended the contract with three one-year renewal options. The contractor is reimbursed for all direct operating costs and is paid an indirect cost fee and a management fee. The contract required all direct operating costs to be properly supported and allowed the College to review and approve such documentation before issuing payment. During fiscal year 2012, according to the College's records, the College paid its food service contractor approximately $4 million.

Recommendation 8

We recommend that the College

a. obtain time summaries supporting all billed labor charges, and

b. ensure that the billed charges are adequately supported prior to payment.

Audit Scope, Objectives, and Methodology

We have audited St. Mary's College of Maryland (the College) for the period beginning April 13, 2009 and ending June 30, 2012. 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 the College'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. The areas addressed by the audit included student accounts receivable, procurements and disbursements, information systems, cash receipts, and payroll. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of the College'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.

The College provides certain support services (such as purchasing, data processing, and maintenance of accounting records) to the Historic St. Mary's City Commission. These support services are included within the scope of our audits of the College. In addition, our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of the College'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 College.

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

The College's response 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 College regarding the results of our review of its response.

APPENDIX

St. Mary's College of Maryland
at Historic St. Mary's City

Office of the Vice President for Business and Finance

November 13, 2013

Thomas J. Barnickel, III, CPA
Legislative Auditor
Department of Legislative Service
Office of Legislative Audits
Maryland General Assembly
301 West Preston Street, Room 1202
Baltimore, Maryland 21201

Dear Mr. Barnickel:

St. Mary's College of Maryland is in receipt of your correspondence dated October 28, 2013 requesting responses to the audit report comments and recommendations. Per your request, we are pleased to submit our responses to each of the eight findings. Please contact me at 240-895-4413, or via email at ccjackson@smcm.edu, with any questions, or if further information is needed.

Regards,

Charles C. Jackson
Vice President for Business and Finance

cc: Ian Newbould, Interim President, St. Mary's College of Maryland
Gail Harmon, Chair, Board of Trustees

Finding 1

The College did not establish independent online approval of certain critical transactions and did not ensure that user access capabilities were properly restricted.

Response: The College agrees with the finding, and will implement the two required changes – by January 1, 2014.

Finding 2

Certain security events were not being logged and monitored and certain individuals could make unauthorized changes to critical programs without detection.

Response: The College agrees with the finding, and has already implemented 8 of the 10 detailed recommendations provided by the OLA audit team regarding this finding. The College expects to complete its implementation of the remaining 2 detailed recommendations – both dealing with improvements in the review of reports that monitor security events – by January 1, 2014.

Finding 3

The College's contract with a cloud service provider did not properly protect the College against certain security and operational risks.

Response: The College agrees with the finding, and discontinued its data backup contract with the cloud service provider in response. If the College contracts with a cloud service provider in the future, it will ensure that the related contract addresses the data security and operational risks identified by the OLA audit team.

Finding 4

The College lacked assurance that all of its active computers were properly protected from malware.

Response: The College agrees with the finding, and has already implemented all 3 of the detailed recommendations provided by the OLA audit team regarding this finding. As a result of these corrective measures, the College now has assurance that all of its active computers are properly protected from malware.

Finding 5

Backup procedures for certain critical servers and network devices did not provide adequate safeguards in the event of a disaster.

Response: The College agrees with the finding, and has already implemented all 3 of the detailed recommendations provided by the OLA audit team regarding this finding. As a result of

these corrective measures, the College's backup procedures for its critical servers and network devices provide adequate safeguards in the event of a disaster.

Finding 6
The College lacked controls to ensure the propriety of refund and non-cash credit transactions.

Response: The College agrees with the finding and will take actions to adequately separate duties such that employees who approve student refunds can't initiate non-cash credit transactions and individuals approving the refund checks perform a documented review of the appropriate supporting documentation. - by January 1, 2014.

Finding 7
Deposit verifications were not documented.

Response: The College agrees with the finding. The verification process agreed to has been implemented.

Finding 8

The College did not sufficiently verify the billings of its food service contractor.

Response: The College agrees with the finding and will obtain time summaries as agreed to at the discussion note stage. We agree to ensure that the billed charges are adequately supported prior to payment. As of November 1 this process is in place.

AUDIT TEAM

Adam J. Westover, CPA
Audit Manager

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

Jonathan H. Finglass, CPA
Senior Auditor

Michael K. Bliss, CISA
John C. Venturella
Information Systems Senior Auditors

Jared J. Bardall
A'knea K. Smith
Tu N. Vuong
Staff Auditors