Audit Report

University System of Maryland
University of Maryland University College

June 2015

OFFICE OF LEGISLATIVE AUDITS

DEPARTMENT OF LEGISLATIVE SERVICES

MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900
Toll Free in Maryland: 1-877-486-9964
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website:

The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

June 8, 2015

Senator Guy J. Guzzone, Co-Chair, Joint Audit Committee
Delegate Craig J. Zucker, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the University System of Maryland (USM) – University of Maryland University College (UMUC) for the period beginning March 21, 2011 and ending June 30, 2014. UMUC offers degree and non-credit educational programs to students who prefer not to enroll in more traditional programs.

Our audit disclosed that security, monitoring, and access controls over the financial and student information systems and related database were not sufficient. For example, unencrypted sensitive personal identifiable information of students, faculty, and staff was stored in the database. In addition, UMUC workstations and servers were not sufficiently protected against malware. Furthermore, agreements which defined the terms and conditions for certain outsourced information technology functions did not address certain security and operational risks.

The USM Office's response to this audit, on behalf of UMUC, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during our audit by UMUC.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

Information Systems Security and Control

Outsourced IT Functions

Background Information

Agency Responsibilities

The University of Maryland University College (UMUC) is a public institution of the University System of Maryland (USM) and operates under the jurisdiction of USM's Board of Regents. UMUC offers degree and non-credit educational programs to students who prefer not to enroll in more traditional programs. UMUC strives to broaden educational opportunities through online education; the majority of UMUC's courses are taught online.

UMUC consists of three major divisions: the Statewide Division, the Asian Division, and the European Division. These three divisions offer educational programs at a number of locations primarily throughout the State of Maryland, as well as in numerous foreign countries. The Statewide Division also administers educational and training programs for adults, and maintains a residential conference center that includes conference rooms, guest accommodations, dining facilities, and an auditorium. UMUC's main administrative office and residential conference center are located in Adelphi, Maryland. The Asian Division is headquartered in Tokyo, Japan and the European Division is headquartered in Kaiserslautern, Germany.

For fiscal year 2014, UMUC's enrollment totaled 84,801 students. UMUC's budget is funded by unrestricted revenues, such as tuition and student fees, a State general fund appropriation, and restricted revenues, such as federal grants. According to the State's accounting records, fiscal year 2014 revenues totaled approximately $372.1 million, which included a State general fund appropriation of approximately $33.7 million.

New Business Model

In February 2015, the USM Board of Regents approved the framework for a new business model for UMUC aimed at addressing its long-term challenges in maintaining its position in a changing global educational marketplace. Under this new model, UMUC would remain within USM but, subject to approval by the Board of Regents, would be granted certain autonomies and exemptions from USM and State laws, rules, and procedures, particularly with regard to personnel, procurement, and the strengthening of protections of proprietary and competitive innovation. The Board supported the appointment of a managing board by UMUC's President and directed the President to develop proposed legislative changes in the Annotated Code of Maryland – State Education Article for review by the Board of Regents and subsequent submission to the Governor and the General Assembly for their consideration. A more developed business model framework is expected to be presented for Board consideration at a future meeting.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the seven findings contained in our preceding audit report dated February 14, 2013. We determined that UMUC satisfactorily addressed these findings.

Findings and Recommendations

Information Systems Security and Control

Background
The University of Maryland University College (UMUC) maintains an internal network and an international wide area network which includes locations in the United States, Europe, and Asia. These locations serve the broader UMUC student body and provide UMUC students with information technology (IT) resources and classroom space.

Over the past few years, UMUC has outsourced many of its critical IT functions, including its financial, student information services and human resources systems, to third-party service providers. These systems are maintained and operated by a combination of service providers and UMUC personnel. In concert with this outsourcing, UMUC has used service providers to host numerous servers used by UMUC to accomplish its core mission requirements. UMUC also maintains numerous workstations and servers in its wide area network. Specifically, as of September 2014 UMUC maintained 235 servers at its main administrative offices in Adelphi and a backup datacenter located in Largo.

Information systems are integral to the UMUC online education function and provide an interactive classroom experience to its students and faculty. Online education services range from supplementing traditional classroom sessions to complete course delivery. In this regard, the online services allow instructors to deliver materials and allow students to submit related class work and interact with classmates and instructors. Online educational courses serve students around the world and account for a significant portion of UMUC's revenues.

Finding 1
Security and access controls over the student information system and a related database were not sufficient.

Analysis
Security and access controls over the student information system and a related database were not sufficient.

- Unencrypted sensitive personal identifiable information (PII) of students, faculty, and staff was stored in the database. We determined that this sensitive PII (social security numbers with related names and birthdates) contained 655,227 unique social security numbers and was stored in 22 different database tables. This sensitive PII, which is commonly sought by criminals for use in identity theft, should be properly protected. The University System of Maryland (USM) *IT Security Standards* require that institutions protect confidential information from disclosure by the deletion of unneeded confidential information, the encryption of confidential information, or other equally secure safeguards.

- A vendor account was assigned the powerful administrator role over the student information system application, although the account did not require administrator capabilities. Accordingly, this vendor (and potentially many of its employees) had full control over the student information system application and its data. USM *IT Security Standards* state that institutions must implement authentication and authorization processes that uniquely identify all users and appropriately control access to systems.

Recommendation 1
We recommend that UMUC

a. **encrypt sensitive PII, including social security numbers, stored in the database; and**
b. **restrict assignment of the student information system application's administrator role to only those individuals who require its use.**

Finding 2
UMUC workstations and servers were not sufficiently protected against malware.

Analysis
UMUC workstations and servers were not sufficiently protected against malware.

- Anti-malware software was not installed on numerous UMUC servers. Specifically, we were advised that 220 servers, running specific operating systems, did not have malware protection software installed. In addition, we tested 10 workstations/servers that had anti-malware software installed and noted in 5 cases the software had not been updated with the latest releases.

- Although UMUC had documented procedures requiring written authorization for users to have administrator rights on their local workstations, we noted that certain workstations were improperly configured with users having administrator rights, without such written authorizations. Administrator rights are the highest permission level that can be granted to users and allow users to install software and change configuration settings. Our test of six workstations disclosed that four employees' user accounts were defined with unauthorized administrator rights, rather than with user rights, and did not need these administrative rights since they were not system/network administrators. As a result, if these workstations were infected with malware, the malware would run with administrative rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights.

- Workstations tested had not all been updated with the latest releases for software products that are known to have significant security software-related vulnerabilities which could be exploited by malware. Although the vendors for these software products frequently provide software patches to address these vulnerabilities, UMUC had not updated its workstations for these patches. For example, we tested eight workstations for one of these software products and noted that four workstations were running older versions of this software.

The USM *IT Security Standards* state that, where feasible, software must be installed to protect the system from malicious programs such as viruses, trojans, and worms.

Recommendation 2
We recommend that UMUC

a. **ensure that all servers and network workstations are configured with anti-malware software that is operating properly and up-to-date;**
b. **ensure that administrative rights on workstations are restricted to system/network administrators and individuals authorized, in writing, to have such rights; and**
c. **keep its workstations up-to-date for all critical security related updates to potentially vulnerable installed software.**

Outsourced IT Functions

Background

As previously mentioned, UMUC has outsourced many of its critical IT functions. In this regard, UMUC entered into service level agreements (which defined the terms and requirements for the contractual services) with service providers for the maintenance and operation of its financial, student information, and human resources systems as well as its mission critical Learning Experience Online (LEO) system which is used to manage and deliver an online learning environment for UMUC students. To provide assurance that the terms of these agreements were complied with, the service providers procured and obtained independent reviews and reports which included descriptions of the service providers' controls and security procedures and the results of tests designed to ensure that these controls and security procedures were effective for designated periods. We reviewed the service level agreements executed with two service providers and independent reports issued for three service providers responsible for the maintenance and operation of LEO and the financial, student information, and human resource systems.

Finding 3
The service level agreements and the related independent reports did not address certain security and operational risks.

Analysis

The service level agreements and the related independent reports did not address certain security and operational risks. Without contractual provisions to address critical security and operational risks, along with comprehensive reviews and reports to ensure the provisions were complied with, UMUC lacked assurance that adequate controls existed to ensure the integrity and availability of its critical systems such as its online learning environment. Specifically, we noted the following conditions:

- For the two service level agreements we reviewed, we noted certain security and operational risks that were not addressed. For example, neither agreement contained a provision to ensure that production data were not replicated in non-production environments. Additionally, one of the two agreements did not contain a provision that required the contractors to perform daily documented reviews of audit logs, which is a best practice identified by the State Department of Information Technology's *Information Security Policy*.

- For the independent reviews and related reports, we noted that certain critical security controls were not addressed. For example, two of the three independent reports we reviewed did not indicate whether intrusion detection, malware prevention, data loss prevention, and antivirus protection controls had been implemented by the service providers. Furthermore, one of these reports also did not indicate if audit logs were reviewed on a regular basis.

We provided UMUC with complete lists of provisions which should be included in the agreements and significant security controls that were not addressed by the independent reviews and reports.

Recommendation 3
We recommend that UMUC

a. attempt to amend the aforementioned existing service level agreements to fully address security and operational risks, including the provisions that we presented to UMUC, and ensure that future service level agreements contain all appropriate provisions; and

b. determine if the independent reviews and related reports address all critical security controls by performing documented reviews of the reports, including ensuring corrective actions are taken regarding issues raised in the reports.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the University System of Maryland (USM) – University of Maryland University College (UMUC) for the period beginning March 21, 2011 and ending June 30, 2014. 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 UMUC's financial transactions, records, and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included purchases and disbursements, student accounts receivable, cash receipts, information systems security and control, payroll, student financial aid, and corporate purchasing cards. We also determined the status of the findings contained in our preceding audit report.

With respect to UMUC's Asian and European Divisions, our audit did not include an evaluation of financial transactions, records, and internal controls and an assessment of compliance with State laws, rules, and regulations. These divisions, which according to UMUC's records, accounted for approximately 5.7 percent and 8.8 percent of UMUC's fiscal year 2014 revenues, respectively, are reviewed on a triennial basis by the USM internal auditors on whose work we relied to reduce the scope of our audit work. In addition, our audit did not include certain support services provided to UMUC by the USM Office (such as endowment accounting) and by the University of Maryland, College Park (such as certain payroll processing functions) which are included within the scope of those audits. Furthermore, our audit did not include an evaluation of internal controls over compliance with federal laws and regulations for federal financial assistance programs and an assessment of UMUC's compliance with those laws and regulations because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including the components of USM.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of UMUC's operations and tests of transactions. We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data), as well as from the contractor administering the State's Corporate Purchasing Card Program (credit card activity). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these various sources were sufficiently reliable for the purposes the data were used during this audit. We also extracted data from UMUC's financial system for the purpose of testing certain information, such as student accounts receivable and financial aid. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

UMUC'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 related to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect UMUC'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 UMUC that did not warrant inclusion in this report.

The response from the USM Office, on behalf of UMUC, 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

UNIVERSITY SYSTEM OF MARYLAND

OFFICE OF THE CHANCELLOR

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

May 27, 2015

Mr. Thomas J. Barnickel III, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, MD 21201

Re: University System of Maryland – University of Maryland University College
Period of Audit: March 21, 2011 through June 30, 2014

Dear Mr. Barnickel:

I have enclosed the University System of Maryland's responses to your draft report covering the examination of the accounts and records of the University System of Maryland – University of Maryland University College. Our comments refer to the individual items in the report.

Sincerely yours,

WE Kirwan

William E. Kirwan
Chancellor

Enclosures

cc: Mr. Javier Miyares, President, UMUC
Mr. George A. Shoenberger, CBO and Vice President, UMUC
Mr. Eugene D. Lockett, Jr., Vice President and CFO, UMUC
Mr. Richard A. Kruckow, Jr., Asst. Vice President and Controller, UMUC
Mr. James L. Shea, Chair, University System of Maryland Board of Regents
Mr. Anwer Hasan, Chairman, MHEC
Ms. Jennie C. Hunter-Cevera, Ph.D., Acting Secretary of Higher Education, MHEC
Mr. Robert L. Page, Associate Vice Chancellor for Financial Affairs, USM Office
Mr. David Mosca, Director of Internal Audit, USM Office

RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE
MARCH 21, 2011 TO JUNE 30, 2014

Information Systems Security and Control

Finding 1
Security and access controls over the student information system and a related database were not sufficient.

Recommendation 1
We recommend that UMUC

- **a. encrypt sensitive PII, including social security numbers, stored in the database; and**
- **b. restrict assignment of the student information system application's administrator role to only those individuals who require its use.**

__University response__

UMUC appreciates OLA's focus on PII and thorough review of the student information system portal database. Security of student information is paramount at UMUC. Accordingly, UMUC adheres to the USM IT Security Standards for protecting data and currently complies with Version 3.0, Section III.3, which states: "Protection measures can include the deletion of unneeded confidential information, the encryption of confidential information, or other equally secure safeguards." While during the audit period, UMUC did not encrypt this database, UMUC did ensure "other secure safeguards" via 1.) routine risk-based assessments, 2.) secure network configurations, 3.) vulnerability scanning, 4.) logging & monitoring, 5.) regular patching & maintenance, and 6.) strong logical and physical access controls, that ensure compliance with USM standards and industry best practices.

OLA accurately identified a second vendor account with administrative privileges for UMUC's student information system during audit fieldwork. The following rationale was shared with OLA during the audit.

In January 2013, UMUC experienced degraded performance with its student information system. Expert analysis and troubleshooting determined that isolation of this issue required a temporary account with system administrator privileges. The single unique account, cited by OLA as evidence for this finding, was:

- created and used with explicit approval from UMUC,
- granted the necessary level of access privileges to perform the work required,
- used by UMUCs' third-party security staff for two (2) days in January 2013, and
- used to successfully rectify the issue.

UMUC appreciates OLA's focus on PII and values Recommendation 1. As a result, UMUC:

a. is implementing Recommendation 1a with a target completion date of 8/31/15,
b. will continue to adhere to the account management policy defined by USM standards.

Finding 2
UMUC workstations and servers were not sufficiently protected against malware.

Recommendation 2
We recommend that UMUC

a. ensure that all servers and network workstations are configured with anti-malware software that is operating properly and up-to-date;
b. ensure that administrative rights on workstations are restricted to system/network administrators and individuals authorized, in writing, to have such rights; and
c. keep its workstations up-to-date for all critical security related updates to potentially vulnerable installed software.

<u>**University response**</u>

The servers in one of UMUC's environments are running a specific operating system and are configured and operating effectively with current, vendor supported anti-malware software. A different UMUC server environment, running another operating system, does not have anti-malware software installed due to a diligent risk analysis. Instead, UMUC uses an industry standard defense-in-depth strategy with controls that mitigate the risk of virus infections and software vulnerabilities, including:

- host-based Intrusion Prevention System (HIPS),
- weekly vulnerability scanning, and integrity monitoring.

UMUC appreciates and wholeheartedly agrees with OLA's analysis and recommendation regarding Local Administrator Rights. As evidence, UMUC implemented a global procedure to restrict these rights on 8/20/14. The procedure, Requesting Local Admin Rights, allows local administrator rights by exception only, with documented approval by responsible parties.

OLA accurately observed multiple versions of a software product in UMUC's environment during audit fieldwork because UMUC was in the process of replacing that product at the time. UMUC stopped purchasing client-based licenses of this product in FY ’14 because the vendor no longer provided updates for this software. As a result, UMUC replaced the unsupported client-based product with the vendor’s cloud solution and was in the process of migration during the audit fieldwork.

a. UMUC will continue to deploy and maintain servers configured with current, functioning, anti-malware software in one server environment. UMUC will continue to monitor industry standard practices and assess the value of anti-malware strategies for servers running in the other server environment. UMUC will continue to employ its multi-tier security strategy for this environment.[1]
b. UMUC will continue to follow its Requesting Local Admin Rights procedure and restrict workstations provisioned prior to this procedure through IT Service Desk requests and the perpetual computer refresh cycle.
c. UMUC will continue to maintain vendor-supported software and current virus definition files for all workstations, including, but not limited to, centralized security and antivirus solutions.

Outsourced IT Functions

Finding 3
The service level agreements and the related independent reports did not address certain security and operational risks.

Recommendation 3
We recommend that UMUC
a. attempt to amend the aforementioned existing service level agreements to fully address security and operational risks, including the provisions that we presented to UMUC, and ensure that future service level agreements contain all appropriate provisions; and

[1] **<u>Auditor's Comment</u>**: While we recognize that UMUC has implemented certain protections over the aforementioned 220 servers, we believe that these protections do not obviate the need for anti-malware software on these servers. Furthermore, although UMUC is not subject to its oversight, the State of Maryland Department of Information Technology (DoIT), which sets cyber security policy for most State agencies, requires that anti-malware software be installed on all computers. We confirmed with DoIT that this requirement applies to all types of operating systems.

b. determine if the independent reviews and related reports address all critical security controls by performing documented reviews of the reports, including ensuring corrective actions are taken regarding issues raised in the reports.

University response

UMUC values OLA's Analysis of contracted service level agreements and will consider incorporating them in future negotiations. The service level agreements reviewed by OLA are part of task order contracts agreed to in 2012 and subordinate to MEEC and USM negotiated and sponsored master agreements. These contracts:

- Predate the USM IT Security Standards v. 3.0 from June 2014, which introduce Section XI. Cloud Computing Technologies. This section outlines risk assessment activities during the preliminary, initiating/coincident, and concluding phases of the lifecycle of the service. Nonetheless, UMUC complied with these standards when the contracts were authored in 2012, during the audit period, and continues to comply today.
- Contain the following language:
    - "Contractor shall (i) establish and maintain industry standard technical and organizational measures to help to protect against accidental damage to, or destruction, loss, or alteration of the material (ii) establish and maintain industry standard technical and organizational measures to help to protect against unauthorized access to the Services and materials; and (iii) establish and maintain network and internet security procedures, protocols, security gateways and firewalls with respect to the Services."
    - "Contractor will take industry standard measures to protect the security and confidentiality of such information including controlled and audited access to any location where such confidential and proprietary data and materials reside while in the custody of Contractor and employing security measures to prevent system attacks (e.g., hacker and virus attacks)."

UMUC's posture and OLA's Analysis are aligned. As such, UMUC's Vendor Risk Management program complies with the current USM Cloud Computing Technology Standard, which outlines activities that consider the security and privacy controls of a cloud provider's environment and assesses the level of risk involved with respect to the control objectives of the organization. UMUC's Vendor Risk Management Program includes, but is not limited to the following activities:

- Thorough review of Statement of Works with UMUC's Procurement and Strategic Contracting Departments and drafting security requirements specific for each vendor solicitation;
- Requiring prospective technology vendors to submit their third-party assessments (SSAE16, SOC 1, 2 Type 1, 2, PCI compliance, and/or other reports) initially and on an annual basis;
- Live vendor presentations/demonstrations where additional security/compliance questions are asked as needed;
- Review of submitted proposals to determine if security requirements are met;
- Administering UMUC's Third Party Security Assessment questionnaire which was developed based on the controls outlined in ISO27002 and NIST 800-53, Rev. 4. The questionnaires may be customized based on the type of product/service offering and UMUC's needs regarding Confidentiality, Integrity, and Availability;
- Reviewing responses to UMUC's questionnaire, as well as the vendor's third-party assessments, asking additional follow-up questions as needed

UMUC appreciates OLA's review of this area and their thoughtful recommendations. UMUC reviews all contracts on a periodic basis for several factors, including security, and when appropriate, UMUC negotiates contract amendments. UMUC also continuously reviews its vendor risk management program and will consider OLA's recommendations for subsequent iterations.

a. UMUC assessed and accepted the existing service level agreements during negotiations and therefore does not intend "to amend the aforementioned existing service level agreements to fully address security and operational risks presented" by OLA at this time. UMUC may amend service level agreements in the future at its discretion.

b. UMUC has reviewed and deemed acceptable the independent reviews and related reports referenced by OLA. Therefore, UMUC does not intend to perform additional documented reviews of these reports at this time. UMUC will continue to receive and review these reports on an annual basis, follow up on any issues with its vendors, and may perform additional reviews in the future at its discretion.

Audit Team

William R. Smith, CPA
Audit Manager

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

Menachem Katz, CPA
Senior Auditor

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

Charnelle S. Brown
Lisa M. DeCarlo
Philip C. Funkhouser
Staff Auditors

Matthew D. Walbert
Information Systems Staff Auditor