Office of Internal Audit

General Information Technology Controls Follow-up Review

May 19, 2015

Internal Audit Team

Shannon B. Henry
Chief Audit Executive

Stacy Sneed
Audit Manager

Rod Isom
Auditor

Winston-Salem State University / **University of North Carolina School of the Arts**
Office of Internal Audit & Institutional Compliance

601 S. Martin Luther King Jr. Drive
Winston-Salem, North Carolina 27110
phone 336.750.2065 | fax 336.750-8891
www.wssu.edu | *www.uncsa.edu*

May 19, 2015

Elwood L. Robinson, Ph.D., Chancellor
Winston-Salem State University
200 Blair Hall
Winston-Salem, NC 27110

Dear Chancellor Robinson:

The following report represents the Office of Internal Audit's second follow-up to matters noted in a confidential letter from the Office of the State Auditor (OSA) dated November 30, 2012. The matters identified by OSA were noted as opportunities for improving information technology (IT) controls. These matters were not considered reportable audit findings for the financial statement or federal compliance audits. However, North Carolina General Statute (NCGS) 116-30.1 requires that Winston-Salem State University (WSSU) make satisfactory progress in resolving weaknesses in the internal structure identified by OSA within a three-month period. Our first follow-up report, dated May 23, 2013, revealed the University made satisfactory progress toward resolving the findings. To ensure continued monitoring and resolution of the deficiencies noted in the OSA letter, we have conducted a second follow-up review.

The report contains IT security matters that are not subject to public disclosure under NCGS 132-6.1. Consequently, we have limited the recipients of this document to protect the security of the University's systems and data.

The report includes a restatement of OSA's report, a summary section explaining Internal Audit's current review procedures and conclusions and an up-to-date response and corrective action plan from University management.

Engagements completed by the Winston-Salem State University Office of Internal Audit are conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors.

Respectfully Submitted,

Shannon B. Henry
Chief Audit Executive

cc: Dr. Brenda Allen, Provost and Vice Chancellor for Academic Affairs
Mr. Derrick Murray, Interim Associate Provost and Chief Information Officer
Audit Committee, WSSU Board of Trustees

***MATTERS SUBJECT TO DISCLOSURE UNDER PUBLIC RECORDS LAW**

1. DISASTER RECOVERY PLAN DOES NOT REFLECT CURRENT IT ENVIRONMENT

The University Disaster Recovery Plan does not reflect the current IT environment. Without an up-to-date Disaster Recovery Plan there is an increased risk of data loss and service interruption in the event of an unexpected disaster.

We found that the University has not documented its Disaster Recovery Plan since moving to the Banner hosted environment. We did determine the University is in the process of beginning a formal risk assessment as a first step to develop an updated Disaster Recovery Plan.

The State of North Carolina Statewide Information Security Manual, Section 140101 "Initiating the Business Continuity Plan (BCP) states that:

> Agencies, through their management, must implement and support an appropriate information technology business continuity program to ensure the timely delivery of critical automated business services to the State's citizens. A management team composed of representatives from all the agency organizational areas has primary leadership responsibility to identify information technology risks and to determine what impact these risks have on business operations. Management must also plan for business continuity, including disaster recovery, based on these risks and document continuity and recovery strategies and procedures in a defined business continuity plan that is reviewed, approved, tested and updated on an annual basis.

Recommendation: The University should develop an updated Business Continuity Plan, which includes disaster recovery reflecting the current IT environment and risks. The Business Continuity Plan should be reviewed, approved, tested and updated on an annual basis or whenever significant changes in the IT environment or risks occur.

University Management's Response: We concur with this finding and are in the process of updating our University Disaster Recovery Plan to reflect the current configuration/architecture of our Banner system which is now hosted by UNC General Administration (GA). The updated plan will be completed once additional information is provided by GA.

INTERNAL AUDIT REVIEW OF ACTIONS TAKEN BY WSSU MANAGEMENT:

- In our report of May 23, 2013, we found that the University had documented the Disaster Recovery Procedures for the current Banner hosted environment. Further, the University had completed a detailed gap analysis, a partial risk assessment, and was in the process of completing a comprehensive risk assessment to develop an understanding of the University's IT policies, procedures, and protocols and determine if they were sufficient to mitigate risks and comply with standards and regulatory requirements. The University's plan was to use the information obtained through the gap analysis and risk assessments to update its IT Disaster Recovery Plan. According to the University's Chief Information Officer (CIO), the IT Disaster Recovery Plan was to be updated by December 2013.

We determined the following related to the details mentioned above (as of our report date):

Corrective Actions Implemented by University Management:

- The University has documented a draft IT Disaster Recovery Plan.
- The University has documented a policy regarding the development, testing, and maintenance of its emergency action plans, to include disaster recovery.

Recommendations Not Addressed by University Management:

- OSA recommended that the University develop an updated Business Continuity Plan, which includes disaster recovery reflecting the current IT environment and risks. Further, OSA recommended that the Business Continuity Plan be reviewed, approved, tested and updated on an annual basis or whenever significant changes in the IT environment or risks occur. During our review, we were not provided evidence of an updated Business Continuity Plan inclusive of disaster recovery. Further, there was no evidence that the draft IT Disaster Recovery Plan had been reviewed, approved or tested.

INTERNAL AUDIT OPINION:

It is our opinion that this issue is still only *partially resolved*.

INTERNAL AUDIT RECOMMENDATION:

The University should implement the previous recommendations and complete its Business Continuity Plan, inclusive of disaster recovery reflecting the current IT

environment. Further, the University should implement procedures to ensure the plan is reviewed, approved, tested and updated on an annual basis or whenever significant changes in the IT environment or risks occur.

UNIVERSITY MANAGEMENT'S RESPONSE:

The Office of Information Technology concurs with this finding and has contacted the University of North Carolina General Administration Office (UNCGA) with respect to recent changes in the architecture of our Banner System, now hosted by UNCGA. In an April meeting, a broad plan was outlined to migrate yet again to a new fault tolerant, highly available infrastructure that will provide advanced Disaster Recovery (DR) capability of the hosted Banner system. This represents a second change in the Banner environment since the original 2012 finding. This latest migration is still in the planning phase which is estimated to have an implementation completion date of June 2016. There will be several iterations of the migration which are all expected to strengthen the overall IT DR plan until completion. The campus IT DR plan is affected by the hosted infrastructure because there will be applications that will be affected by the migration. WSSU staff will continue to make updates and modifications until the migration is complete. We are still in a partially resolved phase, but are making progress.

The Office of Information Technology concurs with the recommendation of updating, reviewing, approving, and testing the Business Continuity Plan (BCP) with respect to significant IT environment changes. It is the intention to update the BCP once the updates to the IT DR plan have been completed.

2. INSUFFICIENT COMMUNICATION OF INFORMATION TECHNOLOGY POLICIES

   The University does not have a formal method of communicating Information Technology policies. This increases the risk of employees unknowingly violating the policies.

   We discovered Information Technology policies are posted on the internet, but there has been no formal communication of the policies to faculty/staff and students. If users of technology on campus are not informed of policies and subsequent policy updates, violations of the Information Technology policies are likely to occur.

   The *State of North Carolina Statewide Information Security Manual*, Section ll0101, "Delivering Awareness Programs to Permanent Staff' states the following:

   The senior management of each agency shall lead by example by ensuring that information security is given a high priority in all current and future activities

and initiatives. The agency, through senior management, shall provide regular and relevant information security awareness communications to all staff by various means, which include but are not limited to the following:

- Electronic updates, briefings, pamphlets and newsletters.
- Information security awareness tools to enhance awareness and educate staff on information technology security threats and the appropriate safeguards.
- An employee handbook or summary of information security policies, which shall be formally delivered to and signed by employees before they access agency resources.

Recommendation: The University should establish a formal method of communicating Information Technology policies and updates to the policies to all technology users.

University Management's Response: The University is in the process of implementing a new security awareness program which will require all University employees to acknowledge that they have reviewed all current IT policies. Also, as part of the security awareness program notices will be sent monthly to inform faculty, staff and students of security threats that may pose a risk and the recommended safeguards. We are currently providing security awareness training through our online training system. We will also work with the Office of Legal Affairs to formally communicate updated policies to the campus community as necessary.

INTERNAL AUDIT REVIEW OF ACTIONS TAKEN BY WSSU MANAGEMENT:

- In our report of May 23, 2013, we found that the University's strategy for communicating IT policies and updates to the policies included the following:
  - IT would work with the Office of Human Resources to incorporate the communication of IT policies into the new employee orientation process. All new employees were to be provided with the University's IT policies and required to sign a statement acknowledging their receipt of such policies prior to accessing the University's system resources. This signed statement was to be incorporated into the new employee's personnel file.
  - IT's Deputy CIO would begin providing continuous information security awareness communications to all University employees electronically. The Deputy CIO would also begin providing campus-wide notifications for all IT policy updates.
  - Annually, as part of the University's network access review process, all University employees with system access were to receive a notification via email with a link directing them to review the University's IT policies.

Employees would be required to acknowledge (electronically) their review of the policies and would continue to receive email notifications until such acknowledgement was complete. This automated notification and response system was part of a long-term plan and was expected to be implemented by December 2014.

We determined the following related to the details mentioned above (as of our report date):

Recommendations Not Addressed by University Management:

- OSA recommended that the University establish a formal method of communicating IT policies and updates to the policies to all technology users. While the University has taken steps toward implementing the strategy noted in our report of May 23, 2013, the actions taken were not significant to effectively address the issue and implement a method to communicate IT policies and updates to all technology users.

INTERNAL AUDIT OPINION:

It is our opinion that this issue is still only *partially resolved*.

INTERNAL AUDIT RECOMMENDATION:

The University should implement the previous recommendation and effectively implement a communication plan for IT policies and updates to the policies.

UNIVERSITY MANAGEMENT'S RESPONSE:

Part of a new security awareness program (still in process) requires posting of policies and updates to those policies to faculty and staff. This will be provisioned by August 30, 2015. In addition, we are providing a web link for faculty and staff to read, review and acknowledge acceptable use policies (AUP). This link is currently under construction. We are also currently providing awareness training through our online training system. Finally, the Office of Information Technology plans to establish an IT training and development center which will require all faculty and staff to attend training seminars on updated policies and procedures annually to address this requirement. This action is under development.

***MATTERS NOT SUBJECT TO DISCLOSURE UNDER PUBLIC RECORDS LAW**

This section of the report contains Information Technology (IT) security matters that are not subject to public disclosure under NCGS 132-6.1. Consequently, we have limited the recipients of this information to protect the security of the University's systems and data.