Office of Internal Audit

Business Continuity Management Review

November 14, 2014

Internal Audit Team

Shannon Henry
Chief Audit Officer & Executive Director of Institutional Compliance

Stacy Sneed
Audit Manager

Javon Lee
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

AUDITOR'S TRANSMITTAL

November 14, 2014

Mr. George Burnette, Chief Operating Officer
University of North Carolina School of the Arts
1533 South Main Street
Winston-Salem, NC 27127-2188

Dear Mr. Burnette:

The Office of Internal Audit & Institutional Compliance has completed its audit of the University's Business Continuity Management Program, inclusive of the business continuity, information technology disaster recovery and pandemic plans. Our audit scope included the calendar year 2013; however, we reviewed the University's most recent continuity of operations plans, which were for the fiscal year 2014. The results of our audit, along with recommendations for corrective action and management's responses, are contained in this report. *A separate Management Letter, which includes minor issues and other information considered ancillary, will also be communicated to management.*

Respectfully submitted,

Shannon B. Henry
Chief Audit Officer and Executive Director of Institutional Compliance

cc: Mr. Lindsay Bierman, Chancellor
Mr. Gary Davis, Interim Chief of Police
Ms. Lisa Smith, Chief Information Officer
Ms. Clarisse Davis, Emergency Management Coordinator
Audit Committee, UNCSA Board of Trustees

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The State of North Carolina requires State agencies to ensure that business continuity and disaster recovery plans are developed, maintained and tested on a prescribed basis and subjected to a continual update and improvement process to maintain operations in the event of an emergency, so far as is reasonably practical. Further, in light of the financial and reputational risk associated with disaster and other business disruptions, an audit of the University's Business Continuity Management Program was identified during our annual risk assessment process. Selection of this audit was based upon a comprehensive plan to assess the internal control environment across all divisions of the University of North Carolina School of the Arts.

The objectives of our audit were as follows:

- To ensure that authorized and documented business continuity, disaster recovery, and pandemic plans are created and maintained up-to-date;
- To ensure the plans are adequate and effective to support the prompt recovery of crucial enterprise functions and Information Technology (IT) facilities in the event of major failure or disaster;
- To ensure plans have adequate compliance policies and procedures in place;
- To ensure potential risks to the enterprise, faculty, staff and students, and its IT facilities are identified and assessed in preparation of the plans;
- To ensure that optimum contingency arrangements are selected and cost effectively provided;
- To ensure the recovery plan is periodically tested for its relevance and effectiveness;
- To ensure internal and external parties to the recovery process are fully aware of their responsibilities and commitments;
- To ensure that both the damaged and recovery sites are secure and that systems are securely operated in support of the enterprise;
- To ensure that systems and procedures are adequately and accurately documented to aid in the recovery process; and
- To ensure that public and media relations would be effectively addressed during an emergency in order to minimize adverse publicity and business implications.
- To ensure that procedures are in compliance with statutory requirements and University policies and procedures;
- To ensure that the University's assets are properly safeguarded; and
- To ensure that resources are used efficiently and effectively.

The audit assessed the University's policies and procedures to be used for the recovery of the University's essential and critical business activities in the event of a natural disaster or other disruptive event. The audit examined the IT disaster recovery plan, the pandemic plan and 17 of the 30 documented business continuity plans. The audit included a comparison of the

EXECUTIVE SUMMARY *(concluded)*

University's practices to the State and industry's standards and best practices to determine compliance.

We found that there are documented business continuity, IT disaster recovery, and pandemic plans in place that contain processes for the mitigation of disasters and other business disruptions. Based upon a review of the best practices and policies and procedures of various state and federal agencies and corporations, we determined that the University's Continuity of Operations Plan (COOP) template (provided by the University of North Carolina's General Administration Office) is a good foundation for a business continuity plan.

The audit also identified deficiencies in the practices that need improvement to mitigate the risks of unpreparedness and to ensure compliance with regulations and standards. These items are discussed in the following *Summary of Findings*.

Summary of Findings:

We found that, in some instances, the University's policies and/or procedures for business continuity and disaster recovery are inadequate to ensure effectiveness.

Specifically, we noted:

- The University's plan for IT Disaster Recovery does not address University systems outside of the accounting information system.
- The University does not test the Continuity of Operations Plans (COOPs).

Summary of Recommendations:

- The University should follow best practices and ensure a proper risk assessment is conducted when creating the disaster recovery plan. The University should develop a complete IT disaster recovery plan, in conjunction with its business continuity plans, to ensure there are strategies in place to restore hardware, applications and data in time to meet the needs of business recovery. The University should perform a business impact analysis, prior to development of the disaster recovery plan, to establish priorities and recovery time objectives. The University should strengthen its control structure over its IT disaster recovery by developing and implementing policies and procedures to help ensure management's directives are carried out and that necessary steps to address risks are taken.
- The Department of Public Safety and Emergency Management should work with COOP managers and establish a schedule for departmental testing of COOPs.

INTRODUCTION

The Office of Internal Audit conducted an audit of the University of North Carolina School of the Arts' (UNCSA) Business Continuity Management Program. As part of the University's overall Business Continuity Management Program, the University maintains departmental business continuity plans, a pandemic plan and an information technology (IT) disaster recovery plan.

The Emergency Management Coordinator (EMC) is responsible for maintaining and coordinating updates of the University's continuity of operations plans (COOPs) and the pandemic plan. The EMC is a part of the Department of Police and Public Safety and reports to the Senior Director. Each major department at the University maintains desk copies of their COOP. The Director of Health Services provides guidance for the Pandemic Plan and is the staff member appointed to monitor information from the World Health Organization (WHO) and Center for Disease Control (CDC) on flu activity, up-to-date recommendations, and travel advisories.

The IT disaster recovery plan is maintained by the Office of Information Technology under the leadership of Ms. Lisa Hardin Smith, Chief Information Officer.

The best practice guidelines as per the Business Continuity Institute state:

> Business Continuity Management is a holistic process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

While each of the types of plans maintained by the University are uniquely different in their information and usability, taken together they are pivotal to an organization that desires to remain a viable enterprise if struck by a disruptive event.

The following definitions have been provided to detail the differences between each of the plans:

- **Business Continuity Planning:** A strategic process for the continuation of essential business operations in instances where a natural disaster or other calamity disrupts an organization's critical operations or services. Having a business continuity plan can assist an organization in avoiding escalating and often crippling downtime costs;

- **Disaster Recovery Planning:** The advance planning and preparations that are necessary to minimize loss and recover technology systems that support critical business functions of an organization in the event of a disaster. This is often referred to as the technological aspect of business continuity planning; and

INTRODUCTION *(continued)*

- **Pandemic Planning:** A strategic process for how an organization will continue to provide essential services in the event of a widespread outbreak of a dangerous infectious disease. The plan should specify how the business will minimize the risk of contagion among employees.

The objectives of our audit were as follows:

- To ensure that authorized and documented business continuity, IT disaster recovery, and pandemic plans are created and maintained up-to-date;
- To ensure the plans are adequate and effective to support the prompt recovery of crucial enterprise functions and IT facilities in the event of major failure or disaster;
- To ensure plans have adequate compliance policies and procedures in place;
- To ensure potential risks to the enterprise, faculty, staff and students, and its IT facilities are identified and assessed in preparation of the plans;
- To ensure that optimum contingency arrangements are selected and cost effectively provided;
- To ensure the recovery plan is periodically tested for its relevance and effectiveness;
- To ensure internal and external parties to the recovery process are fully aware of their responsibilities and commitments;
- To ensure that both the damaged and recovery sites are secure and that systems are securely operated in support of the enterprise;
- To ensure that systems and procedures are adequately and accurately documented to aid in the recovery process;
- To ensure that public and media relations would be effectively addressed during an emergency in order to minimize adverse publicity and business implications;
- To ensure that procedures are in compliance with statutory requirements and University policies and procedures;
- To ensure that the University's assets are properly safeguarded; and
- To ensure that resources are used efficiently and effectively.

To conduct our audit we performed the following procedures:

- Interviewed University employees;
- Reviewed applicable governing regulations and University policies;
- Reviewed business continuity, IT disaster recovery, and pandemic plans and plan test results; and
- Reviewed physical and logical security for University information systems at the University and at an off-site storage facility.

INTRODUCTION *(concluded)*

This report presents the results of our audit.

AUDIT FINDINGS AND RESPONSES

The following audit findings were identified during the current audit and describe conditions that could adversely affect the University's ability to meet its internal control and compliance objectives.

FINDINGS:

1. *The University's plan for IT Disaster Recovery does not address University systems outside of the accounting information system.*

The University does not have a complete written IT disaster recovery plan to facilitate recovery of information systems in case of a disaster. Without an adequate plan for IT disaster recovery there is an increased risk that the plan will be nonviable, not reflective of the strategies of the University, and may prolong recovery of operations in the event of disruptions.

The University's Office of Information Technology has a disaster recovery plan for its accounting information system (Banner) to facilitate recovery of its database and applications. Further, we found evidence showing they test the recovery of Banner data. The Office of Information Technology did not, however, provide documentation to support any efforts to identify and evaluate the impact of disasters on IT systems outside of Banner, the priority and steps necessary to recover those systems, or the IT resources required to support time-sensitive business functions and processes if a disaster were to strike. Additionally, we were not able to find evidence of written policies and procedures applicable to the University's IT disaster recovery efforts.

A well thought out disaster recovery plan includes a risk assessment of all critical information technology systems followed by an impact analysis to ensure necessary services are provided in the most effective fashion.

The State of North Carolina Statewide Information Security Manual states:

> *Section 010101* – Each agency, through its management, is required to protect and secure the information under its control. The basic information requirements include, but are not limited to: Maintaining a business and disaster recovery plan with respect to information technology and process.
>
> *Standard 140102* – Agencies shall conduct risk impact analysis activities that include estimating the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact.
>
> *Standard 150101* – The risk management program must identify and classify risks and implement risk mitigation as appropriate. The program must include the identification, classification, prioritization and mitigation processes necessary to sustain the

AUDIT FINDINGS AND RESPONSES *(continued)*

> operational continuity of mission critical information technology systems and resources. Agencies are encouraged to select and use guidelines that support industry best practices for risk management relative to business continuity planning and security as appropriate.

According to best business practices from the CISCO White Paper regarding Disaster Recovery: Best Practices states:

> *Section 1* – Disasters are inevitable but mostly unpredictable, and they vary in types and magnitude. The best strategy is to have some kind of disaster recovery plan in place, to return to normal after the disaster has struck. The disaster recovery plan does not stop at defining the resources or processes that need to be in place to recover from a disaster. The plan should also define how to restore operations to a normal state once the disaster's effects are mitigated. Finally, ongoing procedures for testing and improving the effectiveness of the disaster recovery system are part of a good disaster recovery plan.

Recommendations: The University should follow best practices and ensure a proper risk assessment is conducted when creating the disaster recovery plan. Further, the University should develop a complete IT disaster recovery plan, in conjunction with its business continuity plans, to ensure there are strategies in place to restore hardware, applications and data in time to meet the needs of business recovery. The University should perform a business impact analysis, prior to development of the plan, to establish priorities and recovery time objectives. Finally, the University should strengthen its control structure over its IT disaster recovery by developing and implementing policies and procedures to help ensure management's directives are carried out and that necessary steps to address risks are taken.

University Management's Response: We concur that a business impact analysis is necessary to determine the priorities of campus stakeholders and recovery times for the non-Banner related systems. Documentation is also required to integrate these priorities into the Continuity of Operation Plans maintained by the Emergency Management Coordinator. We will also incorporate our existing vendor and server maintenance agreements for these systems, into a single disaster recovery document representing both Banner and non-Banner services. This comprehensive plan will be set forth in defined procedures and governed by policies as determined by the Chief Information Officer.

2. *Lack of testing of the Continuity of Operations Plans (COOPs).*

The University does not adequately test its COOPs. A lack of routine testing increases the risks of prolonged business disruption, asset loss and injury to students, staff, and faculty.

AUDIT FINDINGS AND RESPONSES *(continued)*

UNCSA has COOPs for approximately thirty departments. We reviewed seventeen out of the thirty (57%) and found that the Department of Police and Public Safety was the only department that had taken any action relative to testing during our audit period. The department held both an emergency preparedness tabletop and an active shooter exercise in 2013. These two exercises tested the emergency preparedness of the University; however, they did not cover testing of the individual COOPs.

To ensure effectiveness, departmental COOPs should be validated through testing or practical application. It is not enough to make sure that plans are updated and maintained; testing is the only way to determine plan viability. Further, testing ensures the individuals responsible for people, property, and data have an understanding necessary to execute the plans in the event of an actual emergency for effective safeguarding.

UNCA's comprehensive COOP explains that one of the objectives of the COOP is "To establish University requirements for regularly scheduled testing, training, and exercising of department personnel, equipment, systems, processes and procedures used to support University operations during a COOP event." The COOP states further that, "University departments will also test their individual plans, including backup and recovery systems, on a regular basis as a part of their normal operating procedures. It is through such testing that gaps may be identified and modifications made."

FEMA Best Practices notes the benefits of training and exercises for business continuity plans, per the following:

> *"Testing & Exercises"* – You should conduct testing and exercises to evaluate the effectiveness of your preparedness program, make sure employees know what to do and find any missing parts. There are many benefits to testing and exercises:
>
> - Train personnel; clarify roles and responsibilities;
> - Reinforce knowledge of procedures, facilities, systems and equipment;
> - Improve individual performance as well as organizational coordination and communications;
> - Evaluate policies, plans, procedures and the knowledge and skills of team members;
> - Reveal weaknesses and resource gaps;
> - Comply with local laws, codes and regulations; and
> - Gain recognition for the emergency management and business continuity program.

Recommendations: The Department of Public Safety and Emergency Management should work with COOP managers and establish a schedule for departmental testing of COOPs.

AUDIT FINDINGS AND RESPONSES *(concluded)*

University Management's Response: The audit finding stated lack of testing of the Continuity of Operations Plans and recommended that the Department of Police and Public Safety should work with COOP managers to establish a schedule for departmental testing. The Department of Police and Public Safety will contract a company that is familiar with the university setting to assist with testing of the departmental COOP's starting with the most critical departments on campus followed by the remaining departments. The company will assist with the logistics, management of the testing, and an evaluation report.

In September, the Emergency Management Coordinator attended an Effective Business Continuity Management course. This course provided an intensive, hands-on workshop covering all major aspects of effective Business Continuity Management. The course also offered "best practices" on how to develop and maintain effective continuity plans and effective ways to test Business Continuity plans.

Unfortunately we do not have adequate staff within the department to follow the ideal annual protocol of testing. We can test about every 2-3 years, given current resources.