Northern Arizona University

Report on Internal Control and on Compliance

Year Ended June 30, 2017

A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

The Auditor General is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits and special reviews of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Senator **Bob Worsley**, Chair

Senator **Sean Bowie**

Senator **Judy Burges**

Senator **Lupe Contreras**

Senator **John Kavanagh**

Senator **Steve Yarbrough** (ex officio)

Representative **Anthony Kern**, Vice Chair

Representative **John Allen**

Representative **Rusty Bowers**

Representative **Rebecca Rios**

Representative **Athena Salman**

Representative **J.D. Mesnard** (ex officio)

Audit Staff

Jay Zsorey, Director

David Glennon, Manager and Contact Person

Contact Information

Arizona Office of the Auditor General
2910 N. 44th St.
Ste. 410
Phoenix, AZ 85018

(602) 553-0333

www.azauditor.gov

TABLE OF CONTENTS

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on internal control over financial reporting and on compliance and other matters based on an audit of basic financial statements performed in accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

The Arizona Board of Regents

We have audited the financial statements of the business-type activities and discretely presented component unit of Northern Arizona University as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise the University's basic financial statements, and have issued our report thereon dated October 20, 2017. Our report includes a reference to other auditors who audited the financial statements of the Northern Arizona University Foundation, the discretely presented component unit, as described in our report on the University's financial statements. We conducted our audit in accordance with U.S. generally accepted auditing standards and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. However, the financial statements of the Northern Arizona University Foundation were not audited in accordance with *Government Auditing Standards*, and accordingly, this report does not include reporting on internal control over financial reporting or instances of reportable noncompliance associated with the Northern Arizona University Foundation.

Internal control over financial reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the basic financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the University's basic financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that have not been identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control, described in the accompanying schedule of findings and recommendations as items 2017-01 through 2017-05, that we consider to be significant deficiencies.

Compliance and other matters

As part of obtaining reasonable assurance about whether the University's basic financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Northern Arizona University's response to findings

Northern Arizona University's responses to the findings identified in our audit are presented in its corrective action plan at the end of this report. The University's responses were not subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we express no opinion on them.

Purpose of this report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the University's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the University's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Debbie Davenport
Auditor General

October 20, 2017

Financial statement findings

2017-01

The University should improve its risk-assessment process over information technology security

Criteria—The University faces risks of reporting inaccurate financial information and exposing sensitive data. An effective internal control system should include an entity-wide risk-assessment process that involves members of the University's administration and information technology (IT) management to determine the risks the University faces as it seeks to achieve its objectives to report accurate financial information and protect sensitive data. An effective risk-assessment process provides the basis for developing appropriate risk responses and should include defining objectives to better identify risks and define risk tolerances, and identifying, analyzing, and responding to identified risks.

Condition and context—The University's annual risk-assessment process did not include an adequate university-wide IT security risk assessment over the University's IT resources, which include its systems, network, infrastructure, and data. Also, the University did not have adequate policies and procedures to identify and classify sensitive information. Further, the University did not evaluate the impact disasters or other system interruptions could have on its critical IT resources and business operations.

Effect—There is an increased risk that the University's administration and IT management may not effectively identify, analyze, and respond to risks that may impact its IT resources.

Cause—The University had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices.

Recommendations—To help ensure the University has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the University needs to improve its University-wide IT risk-assessment process. The information below provides guidance and best practices to help the University achieve this objective.

- **Conduct an IT risk-assessment process at least annually**—A risk-assessment process should include the identification of risk scenarios, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks identified for remediation. An IT risk assessment could also incorporate any unremediated threats identified as part of an entity's security vulnerability scans.
- **Identify, classify, inventory, and protect sensitive information**—Security measures should be developed to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information. Policies and procedures should include the security categories into which information should be classified, as well as any state statutes and federal regulations that could apply, and require disclosure to affected parties if sensitive information covered by state statutes or federal regulations is compromised.

- **Evaluate the impact disasters or other system interruptions could have on critical IT resources**—The evaluation should identify key business processes and prioritize the resumption of these functions within time frames acceptable to the entity in the event of contingency plan activation. Further, the results of the evaluation should be considered when updating its disaster recovery plan.

The University's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-02

The University should improve access controls over its information technology resources

Criteria—Logical access controls help to protect the University's information technology (IT) resources, which include its systems, network, infrastructure, and data, from unauthorized or inappropriate access or use, manipulation, damage, or loss. Logical access controls also help to ensure that authenticated users access only what they are authorized to. Therefore, the University should have effective internal control policies and procedures to control access to its IT resources.

Condition and context—The University did not have adequate policies and procedures to help prevent or detect unauthorized or inappropriate access to its IT resources.

Effect—There is an increased risk that the University may not prevent or detect unauthorized or inappropriate access or use, manipulation, damage, or loss of its IT resources, including sensitive and confidential information.

Cause—The University had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the University needs to develop and implement effective logical access policies and procedures over its IT resources. The University should review these policies and procedures against current IT standards and best practices and implement them university-wide, as appropriate. Further, the University should train staff on the policies and procedures. The information below provides guidance and best practices to help the University achieve this objective.

- **Review user access**—A periodic, comprehensive review should be performed of all existing employee accounts to help ensure that network and system access granted is needed and compatible with job responsibilities.
- **Review contractor and other nonentity account access**—A periodic review should be performed on contractor and other nonentity accounts with access to an entity's IT resources to help ensure their access remains necessary and appropriate.
- **Review all shared accounts**—Shared network access accounts should be reviewed and eliminated or minimized when possible.
- **Manage shared accounts**—Shared accounts should be used only when appropriate and in accordance with an established policy authorizing the use of shared accounts. In addition, account credentials should be reissued on shared accounts when a group member leaves.
- **Review and monitor key activity of users**—Key activities of users and those with elevated access should be reviewed for propriety.

- **Manage employee-owned electronic devices connecting to the network**—The use of employee-owned electronic devices connecting to the network should be managed, including specifying configuration requirements and the data appropriate to access; inventorying devices; requiring security features, such as passwords, antivirus controls, file encryption, and software updates; and restricting the running of unauthorized software applications while connected to the network.

The University's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-03

The University should improve its configuration management processes over its information technology resources

Criteria—A well-defined configuration management process, including a change management process, is needed to ensure that the University's information technology (IT) resources, which include its systems, network, infrastructure, and data, are configured securely and that changes to these IT resources do not adversely affect security or operations. IT resources are typically constantly changing in response to new, enhanced, corrected, or updated hardware and software capabilities and new security threats. The University should have effective written configuration management internal control policies and procedures to track and document changes made to its IT resources.

Condition and context—The University has written policies and procedures for managing changes to its IT resources; however, they were not fully implemented as of fiscal year-end. Also, the University did not have policies and procedures to ensure all IT resources were configured securely.

Effect—There is an increased risk that the University's IT resources may not be configured appropriately and securely and that changes to those resources could be unauthorized or inappropriate or could have unintended results without proper documentation, authorization, review, testing, and approval prior to being applied.

Cause—The University made significant changes to its configuration management policies and procedures but had not fully implemented all of these changes as of fiscal year-end. Further, the University had not reviewed all of its policies and procedures to ensure they were in line with current IT standards and best practices.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the University needs to review its configuration management policies and procedures against current IT standards and best practices, update them where needed, and implement them University-wide, as appropriate. Further, the University should train staff on the policies and procedures. The information below provides guidance and best practices to help the University achieve this objective.

- **Establish and follow change management processes**—For changes to IT resources, a change management process should be established for each type of change, including emergency changes and other changes that might not follow the normal change management process. Further, all changes should follow the applicable change management process and should be appropriately documented.
- **Review proposed changes**—Proposed changes to IT resources should be reviewed for appropriateness and justification, including consideration of the change's security impact.

- **Document changes**—Changes made to IT resources should be logged and documented, and a record should be retained of all change details, including a description of the change, the departments and system(s) impacted, the individual responsible for making the change, test procedures performed and the test results, security impact analysis results, change approvals at each appropriate phase of the change management process, and a post-change review.
- **Roll back changes**—Roll-back procedures should be established that include documentation necessary to back out changes that negatively impact IT resources.
- **Test**—Changes should be tested prior to implementation, including performing a security impact analysis of the change.
- **Separate responsibilities for the change management process**—Responsibilities for developing and implementing changes to IT resources should be separated from the responsibilities of authorizing, reviewing, testing, and approving changes for implementation or, if impractical, performing a post-implementation review of the change to confirm the change followed the change management process and was implemented as approved.
- **Configure IT resources appropriately and securely, and maintain configuration settings**—Configure IT resources appropriately and securely, which includes limiting the functionality to ensure only essential services are performed, and maintain configuration settings for all systems.
- **Manage software installed on employee computer workstations**—For software installed on employee computer workstations, policies and procedures should be developed to address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.

The University's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-04

The University should improve security over its information technology resources

Criteria—The selection and implementation of security controls for the University's information technology (IT) resources, which include its systems, network, infrastructure, and data, are important because they reduce the risks that arise from the loss of confidentiality, integrity, or availability of information that could adversely impact the University's operations or assets. Therefore, the University should implement internal control policies and procedures for an effective IT security process that includes practices to help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources.

Condition and context—The University did not have sufficient written IT security policies and procedures over its IT resources.

Effect—There is an increased risk that the University may not prevent or detect the loss of confidentiality, integrity, or availability of systems and data.

Cause—The University had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the University needs to further develop its IT security policies and procedures. The University should review these policies and procedures against current IT standards and best practices and implement them university-wide, as appropriate. Further, the University should train staff on the policies and procedures. The information below provides guidance and best practices to help the University achieve this objective.

- **Perform proactive logging and log monitoring—**Key user and system activity should be logged, particularly for users with administrative access privileges and remote access, along with other activities that could result in potential security incidents, such as unauthorized or inappropriate access. An entity should determine what events to log, configure the system to generate the logs, and decide how often to monitor these logs for indicators of potential attacks or misuse of IT resources. Finally, activity logs should be maintained where users with administrative access privileges cannot alter them.
- **Prepare and implement an incident response plan—**An incident response plan should be developed, tested, and implemented for an entity's IT resources, and staff responsible for the plan should be trained. The plan should coordinate incident-handling activities with contingency-planning activities and incorporate lessons learned from ongoing incident handling in the incident response procedures. The incident response plan should be distributed to incident response personnel and updated as necessary. Security incidents should be reported to incident response personnel so they can be tracked and documented. Policies and procedures should also follow regulatory and statutory requirements, provide a mechanism for assisting users in handling and reporting security incidents, and making disclosures to affected individuals and appropriate authorities if an incident occurs.
- **Provide training on IT security risks**—A plan should be developed to provide continuous training on IT security risks, including a security awareness training program for all employees that provides a basic understanding of information security, user actions to maintain security, and how to recognize and report potential indicators of insider threats. Security awareness training should be provided to new employees and on an on-going basis.
- **Document IT vulnerability scans policies and procedures—**Policies and procedures should address the formal process for performing vulnerability scans of its IT resources on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards for software flaws and improper configuration, formatting procedures to test for the presence of vulnerabilities, measuring the impact of identified vulnerabilities, and approving privileged access while scanning systems containing highly sensitive data. In addition, policies and procedures should require that vulnerability scan reports and results be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with other departments of the entity to help eliminate similar vulnerabilities.
- **Apply patches—**Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available.
- **Protect sensitive or restricted data—**Restrict access to media containing data the entity, federal regulation, or state statute identifies as sensitive or restricted. Such media should be appropriately marked indicating the distribution limitations and handling criteria for data included on the media. In addition, media should be physically controlled and secured until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity consistent with the data's security classification.

The University's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-05

The University should improve its contingency planning procedures for its information technology resources

Criteria—It is critical that the University have contingency planning procedures in place to provide for the continuity of operations and to help ensure that vital information technology (IT) resources, which include its systems, network, infrastructure, and data, can be recovered in the event of a disaster, system or equipment failure, or other interruption. Contingency planning procedures include having a comprehensive, up-to-date contingency plan; taking steps to facilitate activation of the plan; and having system and data backup policies and procedures.

Condition and context—The University's contingency plan lacked certain key elements related to restoring operations in the event of a disaster or other system interruption of its IT resources. Also, although the University was performing system and data backups, it did not have documented policies and procedures for performing the backups or testing them to ensure they were operational and could be used to restore its IT resources.

Effect—The University risks not being able to provide for the continuity of operations, recover vital IT systems and data, and conduct daily operations in the event of a disaster, system or equipment failure, or other interruption, which could cause inaccurate or incomplete system and data recovery.

Cause—The University had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices. Additionally, The University had not updated its incident management plan based on the results of its most recent test of the plan.

Recommendations—To help ensure university operations continue in the event of a disaster, system or equipment failure, or other interruption, the University needs to further develop its contingency planning procedures. The University should review its contingency planning procedures against current IT standards and best practices, update them where needed, and implement them university-wide, as appropriate. The information below provides guidance and best practices to help the University achieve this objective.

- **Update the contingency plan and ensure it includes all required elements to restore operations—**Contingency plans should be updated at least annually for all critical information or when changes are made to IT resources, and updates to the plan should be communicated to key personnel. The plan should include essential business functions and associated contingency requirements, including recovery objectives and restoration priorities and metrics as determined in the entity's business-impact analysis; contingency roles and responsibilities and assigned individuals with contact information; identification of critical information assets and processes for migrating to the alternative processing site; processes for eventual system recovery and reconstitution to return the IT resources to a fully operational state and ensure all transactions have been recovered; and review and approval by appropriate personnel.
- **Test the contingency plan—**A process should be developed and documented to perform regularly scheduled tests of the contingency plan and document the tests performed and results. This process should include updating and testing the contingency plan at least annually or as changes necessitate, and coordinating testing with other plans of the entity such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or tabletop discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. The test results should be used to update or change the plan.

- **Backup systems and data—**Establish and document policies and procedures for testing IT system software and data backups to help ensure they could be recovered if needed.

The University's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

UNIVERSITY RESPONSE

Dr. Steven Burrell
Chief Information Officer
PO Box 5100
Flagstaff, AZ 86011
Steven.Burrell@NAU.edu

NORTHERN ARIZONA UNIVERSITY

November 15, 2017

Debbie Davenport
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Ms. Davenport:

We have prepared the accompanying corrective action plan as required by the standards applicable to financial audits contained in *Government Auditing Standards* and by the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. Specifically, for each finding we are providing you with our responsible officials' views, the names of the contact people responsible for corrective action, the corrective action planned, and the anticipated completion date.

Sincerely,

Steven C. Burrell

Financial Statement Findings

2017-01

The university should improve its risk-assessment process over information technology security

Contact Persons:
Steve Burrell, Chief Information Officer
Michael Zimmer, Associate Director of Information Security

Anticipated completion date: December 31, 2018

Correction Action: Concur. To help ensure the university has adequate policies and procedures to identify, analyze, and respond to risks that may affect IT resources, the university will improve its university-wide IT risk-assessment process and align it with NIST best practices.

2017-02

The university should improve access controls over its information technology resources

Contact Persons:
Steve Burrell, Chief Information Officer
Michael Zimmer, Associate Director of Information Security

Anticipated completion date: December 31, 2018

Correction Action: Concur. To help prevent and detect unauthorized access or use, manipulation, damage, or loss to IT resources, the university will implement effective logical access policies and procedures over its IT resources in alignment with NIST best practices and train faculty and staff on those policies and procedures. The university will utilize the NIST framework to continue enhancing existing access request policy and procedures for enterprise systems.

2017-03

The university should improve its configuration management processes over its information technology resources

Contact Persons:
Steve Burrell, Chief Information Officer
Michael Zimmer, Associate Director of Information Security

Anticipated completion date: December 31, 2018

Correction Action: Concur. To help prevent and detect unauthorized, inappropriate, and unintended changes to IT resources, the university will implement effective configuration management policies and procedures over its IT resources in alignment with NIST best practices and train faculty and staff

on those policies and procedures. The university will continue to enhance existing change management and configuration policy and procedures.

2017-04

The university should improve security over its information technology resources

Contact Persons:
Steve Burrell, Chief Information Officer
Michael Zimmer, Associate Director of Information Security

Anticipated completion date: December 31, 2018

Correction Action: Concur. Policies and procedures that align with NIST best practices and standards are being drafted by the university to improve security over its information technology resources. Existing policies and procedures will continue being enhanced to align with the latest NIST best practices and guidelines.

2017-05

The university should improve its contingency planning procedures for its information technology resources

Contact Persons:
Steve Burrell, Chief Information Officer
Michael Zimmer, Associate Director of Information Security

Anticipated completion date: December 31, 2018

Correction Action: Concur. To help ensure its operations continue in the event of a disaster, system or equipment failure, or other interruption, the university will further enhance its current contingency planning procedures in alignment with NIST best practices.


ARIZONA
Auditor General
Making a Positive Difference