Northern Arizona University

Report on Internal Control and on Compliance

Year Ended June 30, 2018

A Report to the Arizona Legislature

Lindsey A. Perry
Auditor General

ARIZONA
Auditor General
Making a Positive Difference

ARIZONA
AuditorGeneral
Making a Positive Difference

The Arizona Office of the Auditor General's mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, the Office 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

Representative **Anthony Kern**, Chair
Representative **John Allen**
Representative **Rusty Bowers**
Representative **Rebecca Rios**
Representative **Athena Salman**
Representative **J.D. Mesnard** (ex officio)

Senator **Bob Worsley**, Vice Chair
Senator **Sean Bowie**
Senator **Judy Burges**
Senator **Lupe Contreras**
Senator **John Kavanagh**
Senator **Steve Yarbrough** (ex officio)

Audit Staff

Donna Miller, 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

ARIZONA AUDITOR GENERAL
LINDSEY A. PERRY

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

JOSEPH D. MOORE
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, 2018, 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 19, 2018. 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 2018-01 and 2018-02, 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.

Lindsey Perry, CPA, CFE
Auditor General

October 19, 2018

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

Financial statement findings

2018-01

Managing risk

Condition and context—The University's process for managing its risks did not include an adequate university-wide information technology (IT) risk assessment to respond to university-wide IT risks, such as potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction of IT data and systems. Also, it did not include inventorying sensitive information that might need stronger access and security controls and evaluating and determining the business functions and IT systems that would need to be restored quickly if the University were impacted by disasters or other system interruptions.

Criteria—Effectively managing risk at the University includes an entity-wide risk-assessment process that involves members of the University's administration and IT management to determine the risks the University faces as it seeks to achieve its objectives to not only report accurate financial information and protect its IT systems and data but to also carry out its overall mission and service objectives. The process should provide the basis for developing appropriate responses based on identified risk tolerances and specific potential risks to which the University might be subjected. To help ensure the University's objectives can be met, an annual risk assessment should include considering IT risks. For each identified risk, the University should analyze the identified risk and develop a plan to respond within the context of the University's defined objectives and risk tolerances. The process of managing risks should also address the risk of unauthorized access and use, modification, or loss of sensitive information and the risk of losing the continuity of business operations in the event of a disaster or system interruption.

Effect—The University's operations and IT systems and data may be susceptible to unintended and unnecessary risk.

Cause—The University relied on an informal process to manage IT risks. Also, although the University had developed written data classification procedures and had begun the process of inventorying its sensitive data, an entity-wide inventory had not been completed as of fiscal year-end.

Recommendations—The University should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions and IT systems and data. It also should plan for where resources should be allocated and where critical controls should be implemented. To help ensure it has effective entity-wide policies and procedures to achieve these objectives, the University should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. Responsible administrative officials and management over finance, IT, and other entity functions should be asked for input in the University's process for managing risk. The University should conduct the following as part of its process for managing risk:

- Perform an annual university-wide IT risk-assessment process that includes evaluating risks such as risks of inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security.
- Evaluate and manage the risks of holding sensitive information by inventorying the information the University holds to assess where stronger access and security controls may be needed to protect data in accordance with state statutes and federal regulations.
- Evaluate and determine the business functions and IT systems that would need to be restored quickly given the potential impact disasters or other IT system interruptions could have on critical organizational functions, such as student services, and operations, such as payroll and accounting, and determine how to prioritize and plan for recovery.

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

This finding is similar to prior-year finding 2017-01. The University addressed some of the prior-year reported deficiencies by implementing a portion of the recommendations, and those are not included in this finding.

2018-02

Information technology (IT) controls—access, configuration management, security, and contingency planning

Condition and context—The University's control procedures were not sufficiently designed, documented, and implemented to respond to risks associated with its IT systems and data. The University lacked adequate procedures over the following:

- **Restricting access to its IT systems and data—**Procedures did not consistently help prevent or detect unauthorized or inappropriate access.
- **Configuring systems securely—**Procedures did not ensure IT systems were securely configured and configuration changes were adequately managed.
- **Securing systems and data—**IT security procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss.
- **Updating a contingency plan—**Plan lacked key elements related to restoring operations in the event of a disaster or other system interruption.

Criteria—The University should have effective internal controls to protect its IT systems and help ensure the integrity and accuracy of the data it maintains.

- **Logical access controls—**Help to ensure systems and data are accessed by users who have a need, access granted to systems and data is appropriate, and the University monitors and reviews access to key systems and data.
- **Well-defined documented configuration management process—**Ensures the University's IT systems are configured securely and that configuration changes are documented. This helps limit the possibility of an adverse impact on the system security or operations.
- **IT security internal control policies and procedures—**Help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT systems and data.

- **Comprehensive documented and tested contingency plan**—Provides the preparation necessary to place the plan in operation and helps to ensure business operations continue and systems and data can be recovered in the event of a disaster, system or equipment failure, or other interruption.

Effect—There is an increased risk that the University may not adequately protect its IT systems and data, which could result in unauthorized or inappropriate access and the loss of confidentiality and integrity of systems and data. It also increases the University's risk of not being able to effectively continue daily operations and completely and accurately recover vital IT systems and data in the event of a disaster or system interruption.

Cause—The University had not revised its policies and procedures to ensure they adequately restricted access to its IT resources and relied on an informal configuration management process. Additionally, the University made significant changes to its IT security policies and procedures and contingency plan but did not have time to fully implement these changes during the fiscal year.

Recommendations—To help ensure the University has effective policies and procedures over its IT systems and data, the University should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. To help achieve these control objectives, the University should develop, document, and implement control procedures in each IT control area described below:

Access

- Review employee user access ensuring appropriateness and compatibility with job responsibilities.
- Evaluate the use and appropriateness of accounts shared by two or more users and manage the credentials for such accounts.
- Manage employee-owned and entity-owned electronic devices connecting to the University's systems and data.

Configuration management

- Configure IT resources appropriately and securely, manage configuration changes, and maintain configuration settings.
- Manage software installed on employee computer workstations.

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges.
- Prepare and implement a security-incident-response plan making it clear how incidents should be reported and handled.
- Perform IT vulnerability scans and remediate vulnerabilities in accordance with a remediation plan.

Contingency planning

- Update a contingency plan and ensure it includes all required elements to restore critical operations, including being prepared to enable moving critical operations to a separate alternative site if necessary.
- Test the contingency plan.
- Train staff responsible for implementing the contingency plan.

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

This finding includes portions of similar prior-year findings 2017-02 (access), 2017-03 (configuration management), 2017-04 (IT security), and 2017-05 (contingency planning). The University addressed some of the prior-year reported deficiencies by implementing some of the recommendations, and those are not included in this finding.

UNIVERSITY RESPONSE

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

NORTHERN ARIZONA UNIVERSITY

December 14, 2018

Lindsey Perry
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Ms. Perry:

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
Chief Information Officer

Northern Arizona University
Corrective action plan
Year ended June 30, 2018

Financial statement findings

2018-01
Managing Risk

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

Anticipated completion date: March 2019

Corrective Action Plan: NAU has developed and implemented a University-wide, Enterprise Risk Management process that includes evaluating risks associated with IT. This was adopted in Spring 2018 and continued throughout 2018, including a more specific IT Risk Assessment completed in September and October 2018. An Information Security Policy and related Information Technology Risk Assessment standard were published in the University Policy Library in July 2018. A University Risk Committee has met to review these items on a regular basis and will continue to do so. This Committee includes IT representatives to ensure that IT risks are considered and evaluated.

NAU completed the development and implementation of a Data Classification and Handling Policy and set of Data Handling Protocols. The policy and protocols were published February 13, 2018 and revised July 2, 2018. They are published in the University Policy Library. An initial phase 1 of a Data Inventory took place in June and July 2018 with survey results gathered to inform the phase 2 in-depth Data Inventory planned to occur in the first quarter of 2019.

2018-02
Information technology (IT) controls – access, configuration management, security, and contingency planning

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

Anticipated completion date: March 2019

Corrective Action Plan:

NAU has implemented multi-factor authentication for higher risk areas and for users where job responsibilities include handling or processing of sensitive data types. NAU is continuing to implement multi-factor authentication through Q1 and Q2 of 2019 by evaluating other moderate to high risk areas first. NAU is drafting new policies, standards, and procedures for Access Controls, which will include periodic review of user access to ensure appropriate access levels to job responsibilities and the use of shared accounts.

NAU is currently revising, developing, and implementing configuration management policies and procedures that will include managing baseline configurations and changes made to those baselines, services and software, for servers and endpoints.

NAU has completed the development and implementation of an Information Security Policy and related Information Security Standards including an Auditing, Logging, and Monitoring Standard and a Vulnerability Management Standard. The policy and standards were published July 11, 2018 in the University Policy Library and include the recommendations provided.

NAU has completed the development and implementation of an Information Technology Incident Management policy and procedure. The policy and procedure were published in the University Policy Library October 18, 2018. Formal training and testing of the procedures are estimated to be implemented in Q1 2019 in alignment with the contingency plan listed below.

NAU is revising and updating its IT contingency plan which will include elements to restore critical operations, including IT operations, and preparation to enable the move of critical operations to an alternative location if necessary. The plan will involve training and frequent testing in 2019.

ARIZONA
Auditor General
Making a Positive Difference