University of Arizona

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
John Faulk, 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

Report issued separately

Comprehensive Annual Financial Report

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

ARIZONA AUDITOR GENERAL
LINDSEY A. PERRY

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 aggregate discretely presented component units of The University of Arizona 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 24, 2018. Our report includes a reference to other auditors who audited the financial statements of the aggregate discretely presented component units, 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 aggregate discretely presented component units 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 aggregate discretely presented component units.

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*.

The University of Arizona's response to findings

The University of Arizona'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 24, 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 overall risk-assessment process that included identifying, analyzing, and responding to the university-wide information technology (IT) risks, such as potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction of IT data and systems.

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 consideration of IT risks. For each identified risk, the University should analyze the risk and develop a plan to respond to the risk within the context of the University's defined objectives and risk tolerances.

Effect—The University's administration and IT management may put the University's operations and IT systems and data at unintended and unnecessary risk.

Cause—The University had not fully developed or implemented its new comprehensive risk assessment process.

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. Also, the University should perform an annual entity-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.

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 2017-02.

2018-02

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

Condition and context—The University's IT control procedures were not always sufficiently designed, documented, and implemented to respond to risks associated with its IT systems and data. Further, the University did not clearly designate oversight and monitoring responsibilities to ensure that its business units followed university-wide IT policies and procedures. The University lacked adequate procedures over the following:

- **Restricting access to its IT systems and data—**Policies and procedures did not include logging and monitoring users with elevated access to the University's enterprise systems.
- **Securing systems and data—**IT security policies and procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss. Further, procedures did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls.
- **Developing and documenting a contingency plan—**The University lacked a plan for restoring operations in the event of a disaster or other system interruption. Further, the University did not identify 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—The University should have effective internal controls to protect its IT systems and help ensure the integrity and accuracy of the data it maintains. Further, effective oversight and ongoing monitoring activities are crucial for the University to assess the effectiveness of its IT policies and procedures and take necessary remedial action.

- **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.
- **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 completed its process of assigning oversight and monitoring responsibilities for decentralized IT internal controls. In addition, policies and procedures for access, data classification, and security were either still under development, awaiting approval, or not fully implemented. In addition, the University did not perform a business impact analysis because it had not completed its disaster recovery procedures to align with the movement of its enterprise systems into a cloud environment.

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. Further, the University should clearly designate oversight and perform ongoing monitoring activities to ensure its business units follow university-wide IT policies and procedures. To help achieve these objectives, the University should develop, document, and implement control procedures in each IT control area described below:

Access

- Monitor and review key activity of users with elevated access to its enterprise systems.

Security

- Improve IT vulnerability scans and remediate vulnerabilities in accordance with a remediation plan.
- Identify, evaluate, and apply patches in a timely manner.
- Develop, document, and follow a process for awarding IT vendor contracts.
- Implement existing policies for identifying, classifying, inventorying, and protecting sensitive 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.

Contingency planning

- 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.
- Develop and implement a contingency plan and ensure it includes all required elements to restore critical operations.
- Test the contingency plan.
- Train staff responsible for implementing the contingency plan.
- Test backups of systems and data.

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 findings 2017-01 (oversight), 2017-02 (risk assessment), 2017-03 (access), 2017-04 (security), and 2017-05 (contingency planning).

UNIVERSITY RESPONSE

THE UNIVERSITY OF ARIZONA
Financial Services Office

FINANCIAL SERVICES OFFICE
University Services Building, Room 502
888 N Euclid Ave
Tucson, AZ 85719

Ofc: 520-621-3220
Fax: 520-621-7078

www.fso.arizona.edu

November 27, 2018

Lindsey A. 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,

Nicole Salazar
Acting Vice President and Comptroller, Financial Services

Financial Statement Findings

2018-01

Managing risk

Summary Response: The University acknowledges that our IT risk assessment process needs additional work.

A thorough review of risk assessment needs for revising and expanding the current risk assessment process revealed that the use of professional services to complete risk assessments would exceed available budget and would require cost prohibitive annual re-assessments. As an alternative, a plan was developed to identify and provide professional training to risk managers, so they can complete the necessary assessments at a lower cost to the University.

To prepare for the first risk assessment cycle, the Information Security Office (ISO) acquired, installed, and configured software tools to enable inventory of resources and risk assessment. These tools provide central tracking and enable enforcement of completion. Training on properly completing and reporting on risk assessments will be conducted in November and December of 2018. Once risk assessments are completed, risk managers will be guided by the ISO to create security remediation plans guided by our risk-based approach. Revised policies governing enforcement were completed by June 30, 2018 and are pending University leadership final approval.

University Contact Personnel: Lanita Collette, Chief Information Security Officer, The University of Arizona (520) 621-9192

Anticipated Completion Date: Policy approval and first risk assessment cycle to be completed by June, 2019.

2018-02

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

Summary Response:

Oversight and monitoring

The University acknowledges that oversight of technical controls in our distributed computing environment needs improvement. To address this need, the Information Security Office will work with campus leadership to facilitate decentralized IT units' adherence to University IT policy. As part of this program, we are deploying monitoring tools on the UA network that can be leveraged by both central and distributed staff.

Security tools have been deployed to monitor internet and internal network traffic, block known malicious activity, and alert on suspicious activity. The University contracted with a vendor for security operation services to monitor alerts 24/7.

By June 30, 2018, the information security office had grown from two to ten staff members and staff began updating policies, including a policy to address enforcement of required security practices. These policies will be presented to campus leadership in December of 2018 for approval. Staff were also able to deploy a solution for tracking inventory in preparation for risk assessment training in November and December 2018.

All campus units are required to participate in the inventory, to be enforced by the Information Security Office (ISO) supported by departmental leadership, as directed by policy.

Several playbooks were developed and distributed to IT staff to aid in consistent and informed response to information security incidents. Additionally, a security Special Interest Group was formed that has membership from all major campus units. This group enhances information sharing about new solutions released by the ISO and ensures that campus units understand new requirements in proposed policies.

Restricting access to its IT systems and data

The University acknowledges a lack of logging and monitoring of elevated access to enterprise systems and will move forward to develop and implement effective logical access policies and procedures.

The University has produced a draft access control policy, purchased and installed a logging and monitoring solution and was in the process of testing and preparing to ingest log data. Processes and procedures for privileged access management are still under development and may require the acquisition of additional software or services.

Securing systems and data

The University acknowledges the need to improve our information security practices. The University continues to hire and train security staff to improve our capacity and ability to handle monitoring, detection, response, contingency-planning, and recovery/lessons learned. The University has 13 staff positions in place, with one more hire planned. This has greatly increased the ability of the Security Office to perform necessary tasks.

The University has installed and tested a vulnerability management tool. The University has also formed working groups to address revising IT policies and IT contracting issues. A new policy has been drafted in a number of areas including data classification and necessary contract provisions. Ongoing contract management is also included in the overall risk management and assessment guideline.

Developing and documenting a contingency plan

The University has revised and tested its backup procedures to align with the movement of enterprise web applications to cloud services. Procedures are documented and a draft policy has been created. Our cloud service provider has failover and recovery capabilities in the event of a disaster, system or equipment failure, or other interruption. We do use multi-availability zones for our enterprise systems. The University will move forward to address business impacts by identifying critical IT systems that will need to be restored quickly in the event of disruption.

As part of the cloud services functionality, snapshots are taken from production and they are staged in a different environment, validating their viability. Our provider has redundancy and failover built into their network and infrastructure, plus the University has the ability to build the environment from scratch if needed with these snapshots. Documenting of procedures is an on-going effort.

Staff education on the process has also been an on-going effort. Key personnel who are directly involved in the configuration have learned the process. Staff generally have been made aware that the process is now automated within our cloud service. In addition, as of October 2018 we have documented the steps and successfully completed a disaster recovery exercise around our Financial application.

University Contact Personnel: Lanita Collette, Chief Information Security Officer, The University of Arizona (520) 621-9192

Anticipated Completion Date:

Oversight and monitoring

This is an ongoing task; substantial work will be completed each year with the first inventory and assessment cycle completed by June 2019.

Restricting access to its IT systems and data

Policies and procedures will be completed and recommendations for the purchase or development of a privileged account management system will be in place by June 2019.

Securing systems and data

Revised policies including data classification, disaster recovery, vulnerability management, vendor contract language, and other matters were completed by June 30, 2018 and are pending University leadership final approval. Procedures and practice based on the new policies will follow; procedures will be documented by June 30, 2019.

Developing and documenting a contingency plan

Testing has been completed; revisions and additions to procedures to address business impact analysis will be completed by June 30, 2019.

ARIZONA
Auditor General
Making a Positive Difference