University of Arizona

Report on Internal Control and on Compliance

Year Ended June 30, 2019

A Report to the Arizona Legislature

Lindsey A. Perry
Auditor General

ARIZONA AuditorGeneral
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

Senator **Rick Gray**, Chair
Senator **Lupe Contreras**
Senator **Andrea Dalessandro**
Senator **David C. Farnsworth**
Senator **David Livingston**
Senator **Karen Fann** (ex officio)

Representative **Anthony T. Kern**, Vice Chair
Representative **John Allen**
Representative **Timothy M. Dunn**
Representative **Mitzi Epstein**
Representative **Jennifer Pawlik**
Representative **Rusty Bowers** (ex officio)

Audit Staff

Donna Miller, Director
John Faulk, Manager

Contact Information

Arizona Office of the Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018-7271

(602) 553-0333

contact@azauditor.gov

www.azauditor.gov

TABLE OF CONTENTS

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* 1

Schedule of findings and recommendations 3

Financial statement findings 3

University response

Corrective action plan

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, 2019, 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 16, 2019. 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 2019-01 and 2019-02, 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 is responsible for preparing a corrective action plan to address each finding. The University's responses and corrective action plan 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 16, 2019

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

Financial statement findings

2019-01

Managing risk

Condition and context—The University's process for managing and documenting 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. Also, it did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls.

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 consider 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.

Effect—Without correcting these deficiencies, 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 has started to conduct a risk assessment process on its significant enterprise systems that includes implementation of its existing data classification policy. However, time and resource limitations have not allowed the University to fully implement prior-year recommendations to effectively manage IT risk.

Recommendations—The University should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact IT systems and data. It also should plan for where to allocate resources and where to implement critical controls. To help ensure it has effective entity-wide policies and procedures to achieve these objectives, the University should follow guidance from a credible industry source, such as 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 entity-wide IT risk assessment process that includes evaluating and documenting risks and safeguards. Such risks may include 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 identifying, classifying, and 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.

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 2018-01 and 2018-02.

2019-02

Information technology (IT) controls—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:

- **Securing systems and data—**Policies and procedures did not require the logging and monitoring of elevated user activities within the University's enterprise systems.
- **Developing and documenting a comprehensive contingency plan—**Plan lacked restoration processes for 2 of the 4 significant enterprise systems, and a copy of the plan was not readily available outside the IT systems.

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.

- **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—Without correcting these deficiencies, 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/or the loss of confidentiality or 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-created work group has not completed its development of logging and monitoring policies and procedures. Further, due to time and resource constraints, the University completed disaster recovery plans for only 2 of its 4 significant enterprise systems.

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 industry source such as 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:

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges.

Contingency planning

- Develop and implement a contingency plan for the remaining 2 significant University enterprise systems.
- Test the contingency plan.
- Train staff responsible for implementing the contingency plan.
- Maintain a readily accessible copy of the 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 is similar to prior-year finding 2018-02.

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 6, 2019

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,

Nicole Salazar
Vice President, Financial Services

Financial statement findings

2019-01

Managing risk

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

Anticipated Completion Date: June 30, 2020

The university will complete risk assessment processes for all enterprise applications by June 30, 2020 including the identification, inventory and classification of data.

The policy and process designate responsibility for executing the process to Information Owners and Information System Owners and makes the Information Security Office accountable for developing, testing, reviewing, and maintaining a university-wide Information Security Plan that incorporates elements of the security plans created and approved by Information Owners and Information System Owners.

This new process allows for the effective management of information security risk through steps for:

- Data collection, including inventory and classification (by criticality and sensitivity) of information resources, identification of stakeholders (from both business and technical positions in the university) and designation of accountability, and analysis of business impacts.
- Risk assessment, with assessment questions based upon the NIST CSF, incorporating elements of confidentiality, integrity, and availability, and tailored to be more meaningful in the environment of higher education.
- Risk analysis that incorporates insights into business impacts, the threat landscape, and an understanding of the traceability between vulnerabilities and threats, to ensure meaningful and consistent risk ranking.
- Security planning that clarifies and documents explicit decisions (within a risk register), based upon risk tolerances of Information Owners and Information System Owners, related to risk handling including choices to accept, transfer, avoid, or mitigate.

The process has been defined as an ongoing activity, for units, with re-assessment and security plan revision occurring at least annually. Production of the University Security Plan will be an annual occurrence, aligned with the fiscal year.

2019-02

Information technology (IT) controls—security and contingency planning

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

Anticipated Completion Date: Logging and Monitoring is an on-going activity. Contingency planning for the remaining two applications will be completed by June 30, 2020 as well as system activity logging and log monitoring, particularly for users with administrative access privileges.

On August 23, 2019, the Audit, Accountability, and Activity Review Standard took effect. This standard supports the corresponding policy and establishes requirements for:

- Responsibility for ensuring log events are captured and monitored;
- The definition of log collection and aggregation systems;
- The collection and retention of logs; and
- Reporting of logging and monitoring related data to the Information Security Office.

Additionally, Information Security Policy Training is under development and is designed to help stakeholders understand their responsibilities for protecting university data; including their responsibility to support log collection and aggregation and to perform review of reports derived from these logs.

By June 30, 2020 the university will ensure stronger access and security controls are in place to protect data in accordance with State statutes and federal regulations, with essence on individuals with elevated privileges. An annual review will be put in place to ensure access and security controls are in place to protect data.

By June 30, 2020, the university will have developed and documented contingency plans for the remaining two significant university enterprise systems. The university testing of its backup procedures aligns with the movement of enterprise web applications to cloud services. The university will move forward to address the business impacts within the two applications, which were not covered in fiscal year 2019, identifying critical IT systems that will need to be restored quickly in the event of disruption. Documented procedures will be created, staff will be trained, and the university will maintain a readily accessible copy of the plans for all enterprise applications. In addition, 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. 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.

ARIZONA
Auditor General
Making a Positive Difference