University of Arizona

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

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

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 aggregate discretely presented component units of The University of Arizona 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 16, 2017. 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 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*.

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.

Debbie Davenport
Auditor General

October 16, 2017

Financial statement findings

2017-01

The University should strengthen oversight of its information technology internal controls

Criteria—A strong control environment should include a governance structure that provides oversight and requires policies and procedures that are documented, communicated to employees, and consistently applied. In addition, an effective internal control system should include monitoring of internal controls to ensure that employees are following the University's policies and procedures.

Condition and context—The University had policies and procedures over most of its information technology (IT) resources, which include its systems, network, infrastructure, and data. However, the University did not monitor its policies and procedures over its IT resources to ensure that they were established and followed.

Effect—There is an increased risk that the University may not achieve its internal control objectives as they relate to IT security and integrity.

Cause—The University is a complex system of colleges and business units, each with their own IT personnel and IT resources. Although the University centralized some aspects of IT internal controls, it had not clearly designated oversight and monitoring responsibilities for those IT internal controls that were not centralized.

Recommendations—To help ensure that the University maintains a strong control environment and effective internal controls over its IT resources, the University should clearly designate oversight and perform monitoring over its IT internal controls to help ensure that they are in place and followed.

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 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 did not complete its risk-assessment process over its IT resources, which include its systems, network, infrastructure, and data. Also, the University did not always follow its policies 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.

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 developed policies and procedures addressing risk-assessment and data classification but did not have a process in place to ensure they were fully implemented. Additionally, a business impact analysis had not been performed.

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

- **Complete an IT risk-assessment process in accordance with its policies and procedures—**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.
- **Implement its policies and procedures for identifying, classifying, inventorying, and protecting sensitive information—**Security measures should be implemented to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information in accordance with the University's data classification and handling standard.
- **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 University 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.

2017-03

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 enterprise 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 for logging and monitoring users with elevated access within its enterprise systems.

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 established written policies and procedures for logging and monitoring users with elevated access within its enterprise systems. The University was aware that technology is available to assist with this process, but the University is not currently utilizing any of these tools.

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 for logging and monitoring users with elevated access within its enterprise systems. In addition, key activities of users with elevated access should be reviewed regularly for propriety. The University should review these policies and procedures against current IT standards and best practices. Further, the University should train staff on the policies and procedures.

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 enterprise 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 further develop and fully implement internal control policies and procedures for an effective IT security process that include 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 fully implement its existing IT security policies and procedures, and in some cases did not have sufficient written 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 data and systems.

Cause—The University developed some policies and procedures for IT security but did not have a process in place to ensure they were fully implemented, and lacked detailed policies and procedures for some IT security areas.

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 policies and procedures over IT security. 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.

- **Improve its incident response plan—**The incident response plan should be further developed 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. All 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 and require making disclosures to affected individuals and appropriate authorities if an incident occurs.
- **Perform IT vulnerability scans—**A formal process should be developed for vulnerability scans that includes 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, vulnerability scan reports and results should be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with other departments to help eliminate similar vulnerabilities.
- **Protect sensitive or restricted data—**Restrict access to media containing data the University, 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 University's data classification and handling standard.

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 enterprise 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 system and data backup policies and procedures.

Condition and context—Although the University was performing system and data backups, it did not have documented policies and procedures for 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's contingency planning policies and procedures need further development to ensure its disaster recovery efforts can be relied on in the event they are needed.

Recommendations—To help ensure university operations continue in the event of a disaster, system or equipment failure, or other interruption, the University should 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 should review its contingency-planning 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 University's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

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

December 11, 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,

Nicole Salazar
Comptroller

Cc: Lisa Rulney, Associate Vice President, Financial Services

Financial statement findings

2017-01

The University should strengthen oversight of its information technology controls

Summary Response: The University acknowledges that oversight of technical controls in our distributed computing environment needs improvement. To address this need, UA leadership appointed a Chief Information Security Officer to build a University security program, who 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. We also will produce and distribute "playbooks" to assist distributed staff to appropriately and consistently handle security incidents.

University contact personnel:
Lanita Collette, Chief Information Security Officer - University of Arizona (520) 621-9192

Anticipated completion date: This will be a phased in plan, with initial work product being delivered in May 2018, and continued delivery of products through their inclusion into oversight and risk assessment processes that will be iterative and ongoing.

2017-02

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

Summary Response: The University acknowledges that our IT risk assessment process needs additional work. To supplement our current product-specific risk assessments and our annual self-assessment process, we will engage professional services for comprehensive assessments mapped to appropriate compliance standards. We will then begin work on prioritized recommendations from the assessments, including identifying and classifying sensitive information. We will also conduct an evaluation of our disaster recovery plan to ensure that key business needs are prioritized and adequately addressed.

University contact personnel:
Lanita Collette, Chief Information Security Officer - University of Arizona (520) 621-9192

Anticipated completion date: This will be a phased in plan, with initial work product being delivered in May 2018, and continued delivery of products through their inclusion into oversight and risk assessment processes that will be iterative and ongoing.

2017-03

The University should improve access controls over its information technology resources

Summary Response: 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.

University contact personnel:
Lanita Collette, Chief Information Security Officer - University of Arizona (520) 621-9192

Anticipated completion date: December 2018

2017-04

The University should improve security over its information technology resources

Summary Response: The University acknowledges the need to improve our information security practices. The University currently plans to hire additional personnel to appropriately staff the Information Security Office. Once hiring and training is complete, we will have improved ability to handle monitoring, detection, response, contingency-planning, and recovery/lessons learned.

University contact personnel:
Lanita Collette, Chief Information Security Officer - University of Arizona (520) 621-9192

Anticipated completion date: May 2018

2017-05

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

Summary Response: We acknowledge that a backup testing plan is necessary as part of the contingency planning and will develop appropriate policies and procedures for testing to ensure successful recovery from backups.

University contact personnel:
Lanita Collette, Chief Information Security Officer - University of Arizona (520) 621-9192

Anticipated completion date: May 2018


ARIZONA
Auditor General
Making a Positive Difference