A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Yavapai County Community College District

Year Ended June 30, 2014

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

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 of school districts, state agencies, and the programs they administer.

The Auditor General's reports are available at:

www.azauditor.gov

Printed copies of our reports may be requested by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Yavapai County Community College District
Report on Internal Control and Compliance
Year Ended June 30, 2014

Table of Contents

Report Issued Separately

Comprehensive Annual Financial Report

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 Governing Board of
Yavapai County Community College District

We have audited the financial statements of the business-type activities and discretely presented component unit of Yavapai County Community College District as of and for the year ended June 30, 2014, which collectively comprise the District's basic financial statements, and have issued our report thereon dated December 12, 2014. Our report includes a reference to other auditors who audited the financial statements of the Yavapai College Foundation, the discretely presented component unit, as described in our report on the District'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 Yavapai College 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 noncompliance associated with the Yavapai College Foundation.

Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered the District'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 District's internal control. Accordingly, we do not express an opinion on the effectiveness of the District's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph 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 were not identified. However, as described in the accompanying Schedule of Findings and Recommendations, we identified certain deficiencies in internal control that we consider to be material weaknesses.

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 District's basic financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying Schedule of Findings and Recommendations as items 2014-01, 2014-02, and 2014-03 to be material weaknesses.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the District'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.*

Yavapai County Community College District's Response to Findings

Yavapai County Community College District's responses to the findings identified in our audit are presented on pages 7 through 9. The District'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 District'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 District's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Jay Zsorey, CPA
Financial Audit Director

December 12, 2014

Yavapai County Community College District
Schedule of Findings and Recommendations
Year Ended June 30, 2014

2014-01

The District should improve access controls over its information systems

Criteria: The District's information technology (IT) systems process and store information and data that is vital to its daily operations. Therefore, the District should have adequate written internal control policies and procedures to control access to its IT systems, including its network, system software, and system information and data.

Condition and context: The District did not have adequate policies and procedures in place to limit logical access to its IT systems. Specifically, auditors noted that there were inappropriate generic access accounts, a large number of administrator access accounts that various employees could use, and terminated employees who could still gain access to the District's network. In addition, one financial system user was found to have excessive access that exceeded what was needed to perform his job duties. Also, the District did not always retain documentation for granting system access, ensuring that the authorized access was compatible with an employee's job responsibilities, and ensuring that the access granted agreed with the access requested. Further, the District did not have policies and procedures in place for removing access or monitoring user activities, including those users with elevated system access, and for periodically reviewing user access to ensure access is needed and compatible with employees' job responsibilities. Finally, the District did not have adequate written policies and procedures for password protection for its financial information system and network.

Effect: There is an increased risk that the District may not adequately prevent or detect unauthorized access, use, damage, loss, or manipulation of programs, information, data, including sensitive and confidential information and systems.

Cause: The District does not have sufficient policies and procedures and lacked detailed instructions for employees to follow for granting and reviewing access to its IT systems.

Recommendation: To help prevent and detect unauthorized access to its IT systems and network and unauthorized use, damage, or loss of information and data, the District should establish policies and procedures that require:

- Performing a periodic, comprehensive review of all existing employee access accounts to help ensure that IT systems and network access granted is needed and is compatible with employees' job responsibilities.
- Reviewing all generic and administrator accounts on its IT systems to eliminate or minimize their use where possible.
- Documenting all requests and approvals of access granted to its IT systems and network. Access should be based on the employees' job responsibilities.
- Reviewing and monitoring the activity of users with elevated access for propriety.
- Strengthening account passwords.
- Removing employees' IT systems and network access immediately upon their terminations.

2014-02

The District should improve its information systems change management process

Criteria: The District's IT systems process and store information and data that is vital to its daily operations. Therefore, the District should have adequate written internal control policies and procedures to track and document changes made to its IT systems, including its network, system software, and system information and data.

Condition and context: The District did not have adequate written policies and procedures to document, test, review, and monitor modifications made to its IT systems. Specifically, the District's current processes do not prevent or detect unauthorized changes to its IT systems and do not require implemented changes to be evaluated against planned outcomes. While the District has a process to track changes made to its IT systems, all other changes to hardware, software, and the network are currently not tracked and are excluded from the change management process. In addition, the District did not ensure adequate separation of system change management responsibilities so that no one person had complete control over the process. Several users had the ability to approve system changes and implement them in the system without an independent review of the changes. Further, the District's change management process was missing other key components, such as procedures to verify changes were in accordance with best security practices, documentation of emergency and custom changes to its systems, procedures to fix changes that didn't work properly, and including all IT systems in its configuration change management process.

Effect: There is an increased risk that changes to the IT systems and data could go undetected or have unintended results without proper documentation, authorization, review, testing, and approval prior to implementation.

Cause: The District does not have sufficient policies and procedures and lacked detailed guidance for employees to follow for making changes to its IT systems.

Recommendation: To help prevent and detect unauthorized modifications to its IT systems, network, hardware, software, and system information and data, district policies and procedures should include requirements for:

- Tracking and reconciling all changes to IT systems, network, hardware, software, and system information and data.
- Separating the responsibilities for developing and implementing changes from the responsibilities of authorizing, reviewing, testing, and approving changes for implementation.
- Documenting all changes to the IT systems and ensuring that changes are authorized, reviewed, tested, and approved prior to implementation. Also, changes should also be evaluated against planned outcomes.

2014-03

The District should improve its policies and procedures over its information technology systems

Criteria: The District's IT systems process and store information and data that is vital to its daily operations. Therefore, the District should have adequate written internal control policies and procedures over the governance of its IT systems. This would include areas such as accessing and monitoring of the IT network, managing employee-owned electronic devices connecting to the network, managing vendors, IT training, and employee access to the Internet.

Condition and context: The District did not have sufficient written policies and procedures over IT security and management. In addition, these policies and procedures were not consistently communicated to staff and properly monitored to ensure compliance. Specifically, the District did not have adequate policies and procedures for the following:

- Logging and monitoring user activity on its IT systems and networks.
- Monitoring employee-owned electronic devices that access the District's network and data. The District does not have a policy addressing employees using their own electronic device, such as a tablet, computer, or phone to connect to the district network. However, the District allows the use of electronic devices but does not have a process to approve and monitor the use of these devices and does not provide guidance to its employees to ensure they understand what constitutes proper and improper security and use of the devices and the District's information and data.
- Maintaining acceptable use requirements and employee guidelines addressing the security of District's information, data, and resources, such as the Internet and the District's social media pages.
- Providing continuous IT training for the District's IT staff and security awareness training for all district staff.
- Communicating its IT policies and changes in IT policies to its employees.
- Properly managing its IT vendors, such as providing guidance for procurement of IT vendor services that require consideration of IT risks, costs, benefits, and technical specifications; monitoring of vendors to ensure conformance with district contracts; and ensuring sensitive data is properly secured and protected.

Effect: There is an increased risk that unauthorized users or inappropriate access to the network may occur and that confidential information and data may be inappropriately shared or manipulated.

Cause: The District does not have sufficient policies and procedures and lacked detailed instructions for risks that affect IT systems and networks.

Recommendation: To help prevent and detect unauthorized or inappropriate access to its IT systems and network, the District should strengthen its existing information security and management policies and procedures. The District's IT policies and procedures should conform to IT standards and best practices. These procedures should include requirements for:

- Logging and monitoring key activities to ensure that only authorized access is allowed to the District's IT systems and networks, including vendors.
- Monitoring employee-owned electronic devices that access the District's network and system information and data. Developing and maintaining IT security policies that include guidelines for managing personal electronic devices and acceptable use of district IT resources, including the Internet and social media.
- Providing continual training for the District's IT staff, as well as mandatory, periodic, district-wide training for all employees on IT policies and procedures and security awareness.
- Communicating district IT policies and changes in IT policies, when they occur, to all employees.
- Monitoring of IT vendor's performance to ensure conformance with district contracts and securing and protecting sensitive information and data from the IT vendors.

DISTRICT RESPONSE

Yavapai COLLEGE

January 26, 2015

Ms. Debbie Davenport, Auditor General
State of Arizona, Office of the Auditor General
2910 N. 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

The accompanying corrective action plan has been prepared as required by Government Auditing Standards. Specifically, we are providing you with the name of the contact person responsible for the corrective action, the corrective action planned, and the anticipated completion date for the audit findings included in the Schedule of Findings and Recommendations for the fiscal year ended June 30, 2014.

Sincerely,

Clint Ewell, Ed.D.
Vice President, Finance & Administrative Services

Yavapai County Community College District
(Yavapai College)
Corrective Action Plan
Year Ended June 30, 2014

2014-01
The District should improve access controls over its information systems

Patrick Burns, Chief Information Officer
Anticipated completion date: June 2015

Corrective Action Plan:

The District agrees with the findings related to its information systems and concurs with the recommendations. The following remediation efforts are underway: periodic reviews of all users to ensure that only appropriate access is provided; generic and administrator accounts are reviewed, reduced, and are actively monitored; documentation of all access requests and approvals will be recorded and will be germane to job responsibilities; account provisioning and maintenance processes will be updated and passwords will adhere to IT best practices.

2014-02
The District should improve its information systems change management process

Patrick Burns, Chief Information Officer
Anticipated completion date: June 2015

Corrective Action Plan:

The District agrees with the findings related to its information systems and concurs with the recommendations. The following remediation efforts are underway or completed: recommendations were included into the existing change management process for the ERP system including the separation of responsibilities for authorizing, reviewing, testing, approving, and implementing changes; material changes to systems and data (including hardware, software, and network) will be documented and monitored.

2014-03
The District should improve its policies and procedures over information technology

Patrick Burns, Chief Information Officer
Anticipated completion date: June 2015

Corrective Action Plan:

The District agrees with the findings related to its information systems and concurs with the recommendations. IT policies have been updated or created in accordance to the recommendations. The following remediation efforts are underway: enhanced systems are being implemented to monitor/log of key activities to ensure only authorized access; new processes and procedures related to monitoring of employee-owned devices are being implemented; new mechanisms are being developed to deliver training to District employees related to security awareness and IT policies and procedures; new procedures are being developed to ensure continuous IT training for District IT employees; procedures related to IT vendor management are being constructed to further protect the District's data and interests.

Yavapai County Community College District
Report on Internal Control and Compliance
Year Ended June 30, 2014

State of Arizona
Office of the Auditor General