

Yuma/La Paz Counties Community College District (Arizona Western College)

CONCLUSION: Yuma/La Paz Counties Community College District is responsible for preparing its annual financial report and a federal expenditure schedule, maintaining effective internal controls, and being accountable for its use of public monies. Our Office is responsible for auditing the District's financial statements, schedule, and major federal programs annually. A summary of the District's financial statements and federal expenditure schedule is presented below.

Based on our audits, we issued opinions on the District's financial statements and federal expenditure schedule and issued reports on internal control and on compliance over financial reporting and major federal programs. The information in the District's fiscal year 2016 financial statements and schedule is reliable. Our Office identified internal control weaknesses over financial reporting. These findings are summarized on the next page.

Condensed financial information

Statement of net position—This statement reports all of the District's assets, deferred outflows of resources, liabilities, deferred inflows of resources, and net position. Net position is reported in three major categories:

- **Net investment in capital assets**—shows the equity in property, buildings, and equipment.
- **Restricted**—shows the resources that must be used for restricted purposes as specified by donors and other external entities, such as the federal government.
- **Unrestricted**—shows the remaining net position balance after allocating the net investment in capital assets and restricted balances.

Statement of revenues, expenses, and changes in net position—This statement reports all revenues, expenses, and other changes in net position. The increase or decrease in net position indicates whether financial health has improved or deteriorated as a result of current-year activities. Net position increased by \$4.4 million, or 24 percent, in fiscal year 2016.

Federal expenditure schedule—During fiscal year 2016, the District expended approximately \$25.2 million in federal awards, which consisted primarily of student financial assistance. The District's federal award expenditures increased by \$1.1 million, or 4.5 percent, compared to fiscal year 2015.

Statement of net position As of June 30, 2016 (In thousands)

Assets and deferred outflows	
Current and other assets	\$ 40,298
Capital assets, net of depreciation	86,701
Deferred outflows of resources	7,834
Total assets and deferred outflows	134,833
Liabilities and deferred inflows	
Current liabilities	8,284
Noncurrent liabilities:	
Net pension liability	40,216
Other	60,171
Deferred inflows of resources	3,396
Total liabilities and deferred inflows	112,067
Net position	
Net investment in capital assets	27,758
Restricted	5,437
Unrestricted (deficit)	(10,429)
Total net position	\$ 22,766

Statement of revenues, expenses, and changes in net position Year ended June 30, 2016 (In thousands)

Revenues	
Tuition and fees, net of scholarship allowances	\$ 4,352
Property taxes	34,037
State appropriations	3,570
Government grants	24,779
Other revenues	5,446
Total revenues	72,184
Expenses	
Educational and general	55,536
Depreciation	4,444
Other expenses	7,836
Total expenses	67,816
Increase in net position	4,368
Net position—beginning	18,398
Net position—ending	\$22,766

Federal expenditure schedule Year ended June 30, 2016 (In thousands)

Federal grantor agency	
Department of Education	\$24,567
Department of Labor	427
Other	183
Total federal expenditures	\$25,177

Summary of audit findings and recommendations

For the District's financial statement audit, we found internal control weaknesses over the District's financial reporting related to its risk-assessment process and information technology (IT) resources. For the federal compliance audit, we tested two federal programs under the major program guidelines established by the Single Audit Act and reported no weaknesses in internal control or instances of noncompliance over federal programs. Our Single Audit report includes a schedule of findings and questioned costs that contains further details to help the District correct the internal control weaknesses summarized below.

The District should improve its risk assessment process over information technology (IT) security risks—The District's risk assessment process did not include the evaluation of IT security risks, including identifying, classifying information by sensitivity, and developing appropriate measures to protect sensitive information. Further, the District did not perform a business impact analysis to evaluate the impact disasters or other systems interruptions could have on its critical business processes, including prioritizing the resumption of these processes within acceptable time frames.

Recommendations

To help ensure that the District's risk assessment process evaluates IT security risks, the District's administration along with the District's IT management group should conduct an IT risk assessment annually that includes identifying, classifying, and inventorying sensitive information and taking appropriate action to protect sensitive information. Also, the District should conduct a business impact analysis to evaluate the impact that disasters or other system interruptions could have on its critical business processes and prioritize the resumption of these processes with in time frames acceptable to the District. The District should consider the results of its business impact analysis when developing its disaster recovery plan.

The District had inadequate policies and procedures over information technology resources—The District's IT resources, which include its systems, network, infrastructure, and data, are vital to its daily operations. However, the District lacked effective policies and procedures over its IT resources to sufficiently protect and manage access, including preventing, detecting, and responding to unauthorized access, and to track, document, and test IT resource changes. The District also lacked a comprehensive up-to-date disaster recovery plan to provide for the continuity of operations in the event of a disaster, system or equipment failure, or other interruption.

Recommendations

The District should evaluate, update, and implement its policies and procedures over IT resources to ensure they effectively address the following:

- Granting, removing, limiting, and changing employees' logical access to its IT resources and performing a periodic, comprehensive review of all existing employee access accounts to ensure that network and system access granted is needed and compatible with job responsibilities.
- Managing and appropriately restricting employee and entity-owned electronic devices and remote access connecting to the District's network.
- Logging, documenting, and retaining records of all change details, including a description of the change, the departments and systems impacted, the individual responsible for making the change, test procedures, test results, security-impact analysis, and approvals.
- Logging and monitoring key user and system activities.
- Developing a process to perform regularly scheduled tests of the District's disaster recovery plan and document the tests performed and results.
- Developing and documenting procedures for IT system and data backups and testing backups, and moving critical information system operations to a separate alternative site in the event of a disaster, system or equipment failure, or other interruption.