ARIZONA
AUDITOR
GENERAL

Lindsey A. Perry, Auditor General

Melanie M. Chesney, Deputy Auditor General

October 3, 2025

Members of the Arizona Legislature

The Honorable Katie Hobbs, Governor

Governing Board
Sonoita Elementary School District

Daniel Erickson, Superintendent
Sonoita Elementary School District

Transmitted herewith is a report of the Auditor General, *A Performance Audit of Sonoita Elementary School District*, conducted pursuant to Arizona Revised Statutes §41-1279.03. I am also transmitting within this report a copy of the Report Highlights to provide a quick summary for your convenience. The CPA firm Walker & Armstrong conducted this performance audit under contract with the Arizona Auditor General.

This school district performance audit assessed the District's spending on noninstructional areas, including administration, student transportation, food service, and plant operations, and made recommendations to the District to maximize resources available for instruction or other District priorities. As outlined in its response, the District agrees with all the findings and recommendations and plans to implement all the recommendations. My Office will follow up with the District in 6 months to assess its progress in implementing the recommendations. I express my appreciation to Superintendent Erickson and District staff for their cooperation and assistance throughout the audit.

My staff and I will be pleased to discuss or clarify items in the report.

Sincerely,

Lindsey A. Perry

Lindsey A. Perry, CPA, CFE
Auditor General

Sonoita Elementary School District

District had lower spending in most operational areas and its student assessment scores exceeded peer and State averages, but the District lacked some internal controls related to cash handling and expenditures; did not comply with IT security requirements; and failed to oversee transportation services, resulting in increased risks to public monies, sensitive computerized data, and student safety

Performance Audit
A Report to the Arizona Legislature
October 2025
Report 25-211

Walker&Armstrong
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

Walker & Armstrong

CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

September 24, 2025

Lindsey A. Perry, CPA, CFE
Arizona Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Dear Ms. Perry:

We are pleased to submit our report in connection with our performance audit of Sonoita Elementary School District for fiscal year 2023, conducted pursuant to Arizona Revised Statutes §41-1279.03.

As outlined in its response, the District agrees with all the findings and plans to implement all the recommendations.

We appreciate the opportunity to provide these services and work with your Office. Please let us know if you have any questions.

Sincerely,

Walker & Armstrong, LLP

Walker & Armstrong, LLP
Phoenix, Arizona

Report Highlights

Walker&Armstrong
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

Sonoita Elementary School District

District had lower spending in most operational areas and its student assessment scores exceeded peer and State averages, but the District lacked some internal controls related to cash handling and expenditures; did not comply with IT security requirements; and failed to oversee transportation services, resulting in increased risks to public monies, sensitive computerized data, and student safety

Audit purpose

To assess the District's efficiency and effectiveness in 4 operational areas—administration, plant operations and maintenance, food service, and transportation—and its compliance with certain State requirements.

Key findings

- District lacked key internal controls over cash-handling and accounting processes, did not reconcile deposits to supporting documentation, and did not have a process for overseeing the superintendent's travel and other expenditures, increasing the risk for errors, misuse, and fraud.
- District did not limit user access to its cloud-based storage service and failed to detect that an external party had downloaded 728 District documents.
- District lacked adequate IT security controls to review user access, enforce password policies, and safeguard systems and data, and did not have a complete contingency plan, increasing the risk of unauthorized access, data loss, errors, fraud, and operational disruptions.
- District did not ensure its contracted transportation provider complied with transportation laws and regulations nor did it verify student counts and mileage reported to ADE were accurate, increasing the risk of student safety concerns, reporting errors, and fraud.

Key recommendations

The District should:

- Limit accounting system access or implement review processes to detect improper transactions or errors, and establish procedures to reconcile deposits to cash receipts and separate key accounting duties.
- Develop a process to ensure transactions made by the superintendent, including travel requests and credit card expenditures, are approved in advance.
- Implement comprehensive IT procedures to limit user access, enforce strong password and security controls, remove unnecessary accounts, and establish and regularly test a contingency plan to reduce risks of unauthorized access, data loss, and operational disruptions.
- Oversee transportation contractor compliance with transportation laws and regulations and verify the accuracy of information reported to ADE.

See Performance Audit Report 25-211, October 2025, at www.azauditor.gov.

TABLE OF CONTENTS

TABLE OF CONTENTS

Tables

Sonoita Elementary School District—Performance Audit Fiscal Year 2023

October 2025

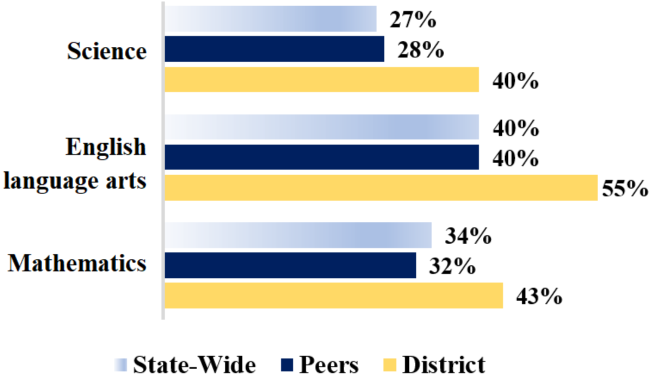
Rural district in Santa Cruz County

Grades: Kindergarten through 8th

FY 2023

- **Students attending: 135**
- **Number of schools: 1**
- **School letter grade[1]: A**

Students who passed State assessments[2]



[1] Source: Arizona State Board of Education 2022-2023.

[2] Source: *Arizona school district spending analysis—Fiscal year 2023.*

FY 2023 total operational spending – $2.45 million ($18,120 per student)

Instructional – 52% ($9,384 per student)	Noninstructional – 48% ($8,736 per student)

Operational overview—FY 2023	Measure	Sonoita ESD	Peer average
Administration—lower per student spending, but improvements needed The District spent less per student on administration than its peer districts averaged, likely due to lower salaries and benefit costs resulting from staff performing duties across multiple operating areas. However, the District lacked important internal controls over cash and did not comply with State conflict-of-interest laws or important IT standards, increasing the risk for errors, misuse, fraud, and data loss (see Findings 1 and 2, pages 3 through 11).	Spending per student	$3,380	$4,259
Plant operations—lower spending and no reported findings The District spent less than its peer districts averaged, likely due to employing fewer personnel to maintain its facilities. We did not report any findings in this area.	Spending per square foot	$8.48	$9.40
	Spending per student	$2,001	$3,000

Operational overview—FY 2023	Measure	Sonoita ESD	Peer average
Food service—lower spending and no reported findings The District spent less on food service than its peer districts averaged, likely due to staff performing duties across multiple operating areas, which allowed their salaries to be allocated across different functions. We did not report any findings in this area.	Spending per meal	$6.83	$7.35
	Spending per student	$972	$1,067
Transportation—higher spending and oversight needed The District spent more on its transportation program than its peer districts averaged, which may be due to its paying 100% of its State transportation funding for outsourced transportation services. Additionally, the District did not properly oversee its transportation contractor, increasing risks of student safety concerns, reporting errors, and fraud (see Finding 3, pages 12 and 13).	Spending per mile	$3.45[3]	$3.12
	Spending per rider	$3,231[3]	$2,243

[3] The District's reported transportation amounts are based on information that the District received from its transportation contractor, but we were unable to validate the figures given the District's lack of supporting documentation.

District lacked important internal controls over cash and some purchases and did not follow requirements in other areas, increasing the risk for errors, misuse, and fraud

Contrary to the USFR, the District did not separate cash-handling and accounting responsibilities and lacked other controls necessary to safeguard cash

Our review found that the District did not comply with the *Uniform System of Financial Records for Arizona School Districts* (USFR) requirements in several areas.[1] Specifically:

- **District did not separate cash handling and accounting responsibilities**—Although the District appeared to have sufficient staffing to comply with USFR requirements to separate responsibilities for receiving cash, initiating payments, and reconciling payments, it had not done so. The USFR requires districts to separate cash-handling responsibilities and establish other safeguards to prevent a single employee from being able to conceal the theft of cash or to complete a transaction, such as a purchase, without independent review or oversight. However, the District had not implemented these safeguards, as described below.
    - The District's process for receiving cash in the mail did not comply with USFR requirements for 2 individuals to open and log the mail and sign off on the log of received items. Without this safeguard, both the business office assistant who collected and distributed the mail, and the business manager who opened the mail, had the ability to misappropriate incoming checks before they were recorded without detection.
    - The District did not conduct independent reconciliations of its cash receipts and deposits. The business manager was responsible for downloading bank statements and preparing bank reconciliations without additional oversight, even though they also had check-signing authority and other cash-handling responsibilities. This could have allowed the business manager to issue fraudulent checks and conceal financial discrepancies without detection.
    - The District's business manager and office assistant both had access to the District's accounting system which gave each of them the ability to initiate and complete purchases without another employee's review or approval, contrary to the USFR.

[1] The Arizona Auditor General and the Arizona Department of Education (ADE) developed the USFR pursuant to Arizona Revised Statutes (A.R.S.) §15-271. The USFR prescribes the minimum internal control policies and procedures to be used by Arizona school districts for accounting, financial reporting, budgeting, attendance reporting, and various other compliance requirements.

Moreover, the business manager had the ability to initiate and complete electronic payments and/or transfers without oversight, which could have allowed for unauthorized or erroneous transactions. For additional information about excessive access to the District's accounting system, see Finding 2, pages 6 through 11.

- **District's reconciliation process did not ensure all monies were deposited**—The District did not reconcile deposits to supporting documentation, such as cash receipts, in accordance with the USFR. We found that although the District's office manager appropriately issued prenumbered receipts when accepting cash payments, the District did not have a reconciliation process to ensure that the amount of cash deposited and recorded in the accounting system matched the amount of cash receipted. Although we did not identify any discrepancies, the lack of reconciliation made it possible for cash collected to be excluded from deposits without detection, increasing the risk of theft.

- **Superintendent's travel and other expenditures lacked oversight**—Contrary to the USFR, the District does not have a process to ensure the superintendent's travel and other credit card expenditures are approved in advance. Additionally, the District did not require staff to separately identify these expenses for the Board's final approval. For instance, when District staff prepare consent agendas summarizing credit card expenditures for the Board's approval, they do not separately identify the charges made by the superintendent, such as for travel expenses, to ensure the Board has the information necessary to exercise proper oversight. By not establishing procedures to ensure that the Board is aware of and approves the superintendent's expenditures and travel, the District increases the risk of misuse or fraud involving its credit cards and/or travel reimbursement process.

Because of the deficiencies in the District's cash receipt and payment processes, we were unable to determine whether all cash received was deposited and disbursements were authorized, as required. When we brought these issues to the District's attention during the audit, District officials stated they were unaware of these deficiencies and would work to develop appropriate controls to address the identified weaknesses.

District employed and paid compensation to a Governing Board member, contrary to State law

Contrary to State laws, in 2022 the District hired a Governing Board (Board) member as a sports coach and paid the Board member compensation totaling $1,600. Statute prohibits an employee of a school district from holding membership on the governing board of the district in which they are employed.[2] District officials indicated they thought Board approval was all that was necessary to employ community members as coaches and they were unaware that Board members were specifically prohibited from being employed by the school districts they oversee. In addition, the District's hiring of a Board member as a sports coach created the potential for a conflict of interest.

Contrary to State conflict-of-interest laws and District policy, the Board member who served as a coach did not disclose their substantial interest on their conflict-of-interest disclosure form nor recuse

[2] A.R.S. §15-421(D) prohibits a school district from employing a governing board member in any capacity.

themselves from Board votes approving the compensation they received for coaching.[3] Specifically, the Board voted in October and December 2022 to authorize coaching stipends, including a total of $1,600 to the Board member who coached for the District. However, the Board member who was to receive the stipends did not recuse themselves from the matter and refrain from participating, as required by law. Additionally, the District's meeting minutes did not document the Board's approval of payments to the Board member or the amounts, as required.

Recommendations

The District should:

1. Develop and implement policies and procedures for cash receipts and disbursements that include: limiting access to the accounting system or implementing a review process to detect improper transactions or errors; reconciling deposits to cash receipts; requiring 2 individuals to open mail and prepare/sign a log of cash receipts; separating duties related to accounting system access, check signing, and bank reconciliations; and requiring dual authorization for bank transfers.

2. Develop and implement policies and procedures to ensure that transactions made by its superintendent, including travel requests, are approved in advance, and ensure that the superintendent's credit card and travel expenses are specifically identified for final Board approval.

3. Immediately terminate the employment of any Board member to comply with State law.

4. Provide additional training to Board members and staff on statutory conflict-of-interest requirements, including employment, disclosure, and recusal obligations, and document the training provided.

District response: As outlined in its response, the District agrees with the finding and will implement the recommendations.

[3] A.R.S. §§38-501 to 38-511.

District's excessive access to its sensitive computerized data and other IT deficiencies increased the risk of unauthorized access to its critical systems and sensitive information, errors, fraud, and data loss

District has not complied with important IT security requirements and credible industry standards

The USFR and credible industry standards, such as those developed by the *National Institute of Standards and Technology* (NIST), set forth important IT security practices that help districts safeguard sensitive information. However, our review of the District's IT security practices identified several deficiencies, including noncompliance with USFR requirements and practices inconsistent with credible industry standards. These deficiencies increased the District's risk for unauthorized access to sensitive information, errors, fraud, and data loss. See the details below.

Deficiency 1: District failed to detect 728 documents downloaded from its data storage service by an external party

The District did not implement security measures for its cloud-based storage service which allowed someone outside the District's domain to download 728 documents without detection. The USFR requires, and credible industry standards recommend, that policies and procedures be implemented to enforce access controls and track and monitor system activity to identify and investigate any unusual behavior. Regular monitoring and auditing allow districts to assess the effectiveness of its security measures in safeguarding sensitive district information.

The District's cloud-based storage service allows administrators to implement access controls, including the ability to control users' ability to share, copy or download documents, but the District had not implemented these measures. Additionally, District officials reported that they believed that the vendor they contract with for certain IT services was responsible for all aspects of the system, including monitoring activity, but that does not appear to be the case. Based on our review of the contract between the District and the external service provider, the vendor was responsible for managing accounts within the cloud-based storage service. These responsibilities included account setup and management, password changes and resets, and all other services related to managing the domain for the District. However, the contract did not specify that the external service provider was responsible for monitoring system activity.

Through our review of the District's October 2024 system activity reports, we identified an incident involving 728 documents being downloaded by an individual who was not employed by the District. A teacher employed by the District shared access to documents with an email address outside the District's domain. We scanned the list of documents downloaded by the external user and identified curriculum-related document names, but we were unable to verify the documents' contents because the District routinely deletes shared document files at the end of each school year. Based on the external user's personal email address and a review of publicly available information, including social media and school district websites, the external user who apparently downloaded the documents appeared to be a teacher at a neighboring school district. District officials reported that prior to our bringing this issue to their attention, they were unaware that a District employee had shared documents with an individual outside the District's domain.

Failure to assign responsibility and implement procedures for monitoring the District's cloud-based storage service increased the risk of unauthorized access to sensitive data, such as student information or personnel records. As of March 2025, District officials reported that they had worked with the District's IT vendor to implement a process for monitoring system activity and had held a meeting with staff members to discuss the incident.

Deficiency 2: District did not regularly review and limit user access to its network and critical systems, increasing its risk of unauthorized access to sensitive information, errors, fraud, and data loss

Our October 2024 review of accounts on the District's cloud-based storage service, student information system (SIS), and accounting information system (AIS) found that the District did not regularly review and limit users' access to critical IT systems in accordance with the USFR and recommended practices (see Table 1, page 8). Specifically:

- **District did not disable user account access after employee termination**—Our review identified 5 IT user accounts that were associated with terminated employees or former contractors that the District had not disabled or removed from its system. Allowing such accounts to remain active is contrary to the USFR requirement to immediately disable system access when it is no longer needed. These accounts, which included 2 with administrator-level access, remained active for between 375 and 479 days after employees or vendors no longer worked for the District. Users with administrator-level access can manage user access and permissions, configure security settings, monitor and modify system activity, grant themselves or others additional system privileges, disable security controls, and access, share, or delete sensitive data. After we brought these accounts to the District's attention, the District disabled them. Although our review did not identify any IT systems that had been accessed by accounts that should have been disabled, the District's failure to remove access when it was no longer needed increased the risk of unauthorized access to sensitive information and data loss.

- **District did not ensure AIS users had only the access necessary to perform their job duties**—Our review found that all 11 users of the AIS had more access than necessary to perform their job duties, contrary to the USFR and credible industry standards. Specifically, each of these 11 AIS users were granted access to the system that allowed them to view and modify employee information and pay rates—including their own—as well as initiate and complete payroll and purchasing transactions without independent review or approval. Ten of these 11 users had full access, including the facilities manager whose job responsibilities only required access to the AIS fixed asset module. Additionally, 1 of these AIS users had administrator-level access in the system, despite not requiring it to perform their job duties. As previously discussed, this level of access allows a user to modify system settings and permissions, including adding, disabling, and changing access for all AIS users.

District officials stated that they were unaware of these access issues prior to our review. Officials explained that due to limited staffing, employees needed access to multiple AIS functions to perform their regular duties, even though these tasks were incompatible and undermined proper separation of duties. However, the District lacked a process for reviewing and assigning system access based on employees' job responsibilities. Further, when proper separation of duties is not feasible due to staffing constraints, the USFR requires districts to implement additional management oversight and compensating controls, such as regular supervisory reviews of transactions, system logs, and activity reports. Although we did not identify any improper transactions due to these deficiencies, system access beyond what is needed for an employee's job duties and failure to remove access when it is no longer needed increases the risk of errors, fraud, and data loss.

Table 1: District did not consistently limit user access to its information systems

Requirement	Cloud-based storage	Student Information System	Accounting Information System	Summary
Limit the number of users with administrator-level access	X	✓	X	We found that the District had 2 users of the cloud-based storage service and 1 user of the AIS system that had administrator access that was not required.
Restrict user access to only include access necessary to perform assigned duties	X	X	X	We found that 5 users of the cloud-based storage service, 2 users of the SIS, and all 11 users of the AIS had more access than was necessary to perform their assigned duties.
Timely remove terminated employees' access	X	X	✓	We found that at least 2 users of the SIS and 5 users of the cloud-based storage service were associated with unidentifiable users or terminated employees.

Source: Walker & Armstrong staff analysis of District information system users' access levels, employment status, and assigned duties for fiscal year 2023 as of October 2024.

Deficiency 3: District did not safeguard its IT infrastructure and sensitive information, increasing its risk for unauthorized access and data loss

Our review of the District's controls found that the District had not implemented essential safeguards which increased the risk of unauthorized access to sensitive information and data loss. Credible industry standards recommend that districts prevent unauthorized access to systems and data by initiating an automatic device lock after a defined period of inactivity or specified number of failed login attempts and that districts backup user level data. Additionally, the USFR requires that districts implement security-related controls over access to IT systems and data. However, the District was missing some of these controls, as discussed below.

- **District devices did not have proper logical access controls**—The District managed user access through local accounts rather than utilizing the centralized directory service available within its operating system, limiting its ability to enforce security settings consistently. The District reported that the absence of centralized management was due to limitations of its operating system. However, the system allows for centralized directory services, but District staff did not understand how to properly configure and implement this functionality. As a result, users were able to customize device settings, including allowing devices to remain unlocked indefinitely and disabling lockout periods after multiple failed login attempts. Additionally, the District lacked policies and procedures to train users on proper logical access controls.

- **District failed to ensure it properly stored sensitive information**—The District relied on a third-party cloud storage service to store and share data files, but it had not trained staff to ensure that all data was properly stored. Cloud-based storage can reduce the risk of data loss and eliminate the need for internal backups, but such a system is only effective if all sensitive records—such as accounting and student information—are stored in the cloud. During our review, we observed that sensitive information was stored on District staff members' local devices instead of the designated cloud storage. Although the District's policy required all data to be stored in the cloud, District staff indicated that they were unaware of how the District's environment was operating and thought that information saved on their individual devices was backed up.

- **District did not safeguard its network**—Our review identified weaknesses in the District's wireless and internal network that could enable access to critical IT infrastructure. The USFR requires that districts implement security-related controls over access to IT systems and data to ensure the data confidentiality and integrity. District staff reported being unaware of these weaknesses and the associated risks and would consult with the District's IT consultant to review and modify the necessary wireless network and infrastructure settings.

Deficiency 4: District's password policy was not enforced, increasing the risks to District data and operations

As previously discussed, the District did not use the centralized directory service within its operating system, so it was unable to enforce a District-wide password policy for all devices. Instead, each individual device required password settings to be manually configured. District staff reported that due to limited staffing, the District was unsure how to configure the password requirement and instead relied on staff to voluntarily adhere to the password policy. However, inquiries of District staff during the audit revealed that they were unaware of the District's password requirements. By not enforcing its password requirements, the District increased the risk that unauthorized individuals could access sensitive District information and disrupt District operations.

Deficiency 5: District lacked a complete IT contingency plan, increasing the risk of data loss and disruptions to operations

To help ensure continued operations and data recovery in the event of a system outage, the USFR requires, and credible industry standards recommend, that districts develop and implement an IT contingency plan, but the District's plan was missing key components. Specifically, the District's IT contingency plan had incomplete, missing, or outdated information for several components, including:

- An impact analysis to assess the likelihood of potential disasters, including possible consequences, and the necessary remedial actions.
- An inventory of IT infrastructure and vital records that would need to be restored, replaced, or recovered in the instance of an incident, and a list of supplies necessary to facilitate recovery efforts.
- Assigned responsibilities for coordinating response efforts, restoring IT systems, and minimizing business disruptions after an event or disaster.
- Documentation of plan maintenance and training on how to identify and respond to emergencies effectively and who to notify in an event or disaster.

We also interviewed 3 district staff with responsibilities outlined in the District's contingency plan and found that 1 of them was unaware of their responsibilities. District staff reported a lack of training on contingency planning, which may have contributed to deficiencies we identified.

In addition to developing and implementing a comprehensive contingency plan, the District should test its plan at least annually to help ensure it is effective. Testing should include ensuring all employees understand their roles and responsibilities, identifying internal and external vulnerabilities, taking action to update equipment or remedy any issues identified, testing its ability to restore electronic data files for critical systems from backups, and documenting the results of the test.

Recommendations

The District should develop and implement written policies and procedures to:

5. Require access controls restricting the ability of users to share, copy, or download documents, and to track and monitor cloud-based storage activity, and investigate any unusual activities that are identified.
6. Assign and periodically review user access to the District's cloud-based storage, accounting information, and student information systems to ensure users have access to only those functions needed to perform their assigned duties. If separation of duties is not feasible due to limited staffing, the District should implement other controls such as a process for a supervisor to regularly review information such as transaction details, system logs, and activity reports, as required by the USFR.
7. Centrally manage user access and enforce security policies across all devices, including strong password requirements that align with credible industry standards.

The District should:

8. Develop and provide training to users on IT security topics, such as password management, session timeouts, login attempt restrictions, and requirements to store all sensitive data on the District's approved cloud-based storage system; and document the training provided.

9. Immediately disable or remove all unnecessary user accounts in its cloud-based storage and student information systems and implement a review process to ensure access to all systems is removed immediately when an employee or vendor service is terminated.

10. Protect sensitive computerized systems and data by evaluating and implementing appropriate security measures for its wireless and internal network.

11. Develop and implement an IT contingency plan that meets USFR requirements and credible industry standards and test the plan at least annually to identify and remedy deficiencies and document the test results.

District response: As outlined in its response, the District agrees with the finding and will implement the recommendations.

FINDING 3

District did not oversee its outsourced transportation services, increasing the risk of student safety concerns, reporting errors, and fraud

The District entered into an intergovernmental agreement (IGA) with a neighboring school district to transport its students to and from school and for activities, but it did not ensure that the transportation services provided complied with State standards and reporting requirements. Statute allows school districts to enter into IGAs with other districts or public agencies to jointly or cooperatively receive or perform needed services.[4] Additionally, in accordance with State procurement rules, school districts may contract with external vendors for goods or services.[5] These requirements and the USFR specify how districts should initiate and oversee agreements and contracts. Proper oversight includes ensuring that goods or services are delivered as required and meet quality standards, evaluating the value of the exchange, and verifying the accuracy of the receipts and payments in accordance with the terms of the agreements and contracts. Further, the District is responsible for ensuring student safety in all aspects of transportation services.

The District's IGA with Patagonia Union High School District (Patagonia UHSD) for transportation services requires Patagonia UHSD to provide the following services: organizing school and extracurricular activity bus routes; supervising transportation employees; administering a random drug testing program for school bus drivers; and supplying and maintaining school bus and fleet vehicles used to transport students. In exchange for these services, the District transfers all transportation funding it receives from the State to Patagonia UHSD. However, the District lacks a process for ensuring Patagonia UHSD complies with DPS *Minimum Standards for School Buses and School Bus Drivers* (Minimum Standards) and other requirements.[6] Specifically:

- **District did not monitor compliance with Minimum Standards to ensure student safety—** Although the IGA required Patagonia UHSD to comply with laws and regulations governing transportation services, the District is responsible for ensuring its students are transported safely. However, the District did not oversee compliance with the IGA's terms to verify that bus drivers held the necessary credentials, were randomly tested for drug and alcohol use, and buses and fleet vehicles were maintained in accordance with Minimum Standards.

- **District failed to verify the accuracy of mileage and rider counts used for funding purposes—**Pursuant to the IGA, Patagonia UHSD provided the District with student rider

[4] A.R.S. §11-952.

[5] A.R.S. §15-213.

[6] Arizona Department of Public Safety (DPS) has established *Minimum Standards for School Buses and School Bus Drivers* (Minimum Standards). Minimum Standards require school districts to perform systematic school bus preventative maintenance, such as brake and tire inspections, safety feature inspections, and oil changes, and maintain records of this preventative maintenance.

counts and route mileage for the District's required State transportation reporting to ADE, which are used to calculate the District's transportation funding amounts. However, our review found that the District could not demonstrate that it had taken steps to verify the accuracy of the information Patagonia UHSD provided to it.

- **District provides 100% of the State transportation funding it receives to Patagonia UHSD, which may not be in the District's best interest—**The IGA requires the District to transfer all transportation funding it receives from the State to Patagonia UHSD for transportation services provided. However, our review of State transportation funding and spending for peer districts found that more than half of the District's peers had funding that exceeded their transportation costs, indicating that these districts were able to use the remaining funding for other district priorities. By revising its IGA to hold back a portion of the transportation funding it receives, the District could potentially offset its costs for overseeing the agreement to better ensure student safety and accurate reporting for funding purposes. In addition, revising its IGA payment terms could potentially reduce any incentives for Patagonia UHSD to over-report mileage and/or riders to obtain money for the transportation services it provides to the District.

District staff reported that they were not aware that oversight was necessary since there was a contractual obligation for Patagonia UHSD to comply with laws and regulations. Consequently, the District had not developed any contract oversight or monitoring procedures. However, without such procedures, the District could not effectively ensure student safety and accurate transportation reporting. Additionally, the District's lack of verification and records prevented us from determining whether the District's transportation program complied with Minimum Standards and whether amounts reported to the State for transportation funding were accurate.

Recommendations

The District should:

12. Develop and implement policies and procedures to oversee and routinely evaluate compliance with transportation laws and regulations for services provided through its transportation IGA, including verifying bus driver credentials, ensuring required drug testing is conducted, and confirming that buses and vehicles used to transport students meet Minimum Standards.

13. Develop and implement a process for routinely verifying the accuracy of student transportation counts and route mileage data provided by Patagonia UHSD before submitting reports to ADE to ensure accurate funding calculations.

14. Evaluate its transportation IGA to determine whether it fully addresses issues such as access to records for compliance reviews and whether changes are warranted to the amount the District pays for transportation services.

15. Develop and provide annual training to responsible District staff on transportation program requirements and oversight responsibilities.

District response: As outlined in its response, the District agrees with the finding will implement the recommendations.

Walker & Armstrong makes 15 recommendations to the District

The District should:

1. Develop and implement policies and procedures for cash receipts and disbursements that include: limiting access to the accounting system or implementing a review process to detect improper transactions or errors; reconciling deposits to cash receipts; requiring 2 individuals to open mail and prepare/sign a log of cash receipts; separating duties related to accounting system access, check signing, and bank reconciliations; and requiring dual authorization for bank transfers (see Finding 1, pages 3 through 5, for more information).

2. Develop and implement policies and procedures to ensure that transactions made by its superintendent, including travel requests, are approved in advance, and ensure that the superintendent's credit card and travel expenses are specifically identified for final Board approval (see Finding 1, pages 3 through 5, for more information).

3. Immediately terminate the employment of any Board member to comply with State law (see Finding 1, pages 3 through 5, for more information).

4. Provide additional training to Board members and staff on statutory conflict-of-interest requirements, including employment, disclosure, and recusal obligations, and document the training provided (see Finding 1, pages 3 through 5, for more information).

5. Develop and implement written policies and procedures to require access controls restricting the ability of users to share, copy, or download documents, and to track and monitor cloud-based storage activity, and investigate any unusual activities that are identified (see Finding 2, pages 6 through 11, for more information).

6. Develop and implement written policies and procedures to assign and periodically review user access to the District's cloud-based storage, accounting information, and student information systems to ensure users have access to only those functions needed to perform their assigned duties. If separation of duties is not feasible due to limited staffing, the District should implement other controls such as a process for a supervisor to regularly review information such as transaction details, system logs, and activity reports, as required by the USFR (see Finding 2, pages 6 through 11, for more information).

7. Develop and implement written policies and procedures to centrally manage user access and enforce security policies across all devices, including strong password requirements that align with credible industry standards (see Finding 2, pages 6 through 11, for more information).

8. Develop and provide training to users on IT security topics, such as password management, session timeouts, login attempt restrictions, and requirements to store all sensitive data on the District's approved cloud-based storage system; and document the training provided (see Finding 2, pages 6 through 11, for more information).

9. Immediately disable or remove all unnecessary user accounts in its cloud-based storage and student information systems and implement a review process to ensure access to all systems is removed immediately when an employee or vendor service is terminated (see Finding 2, pages 6 through 11, for more information).

10. Protect sensitive computerized systems and data by evaluating and implementing appropriate security measures for its wireless and internal network (see Finding 2, pages 6 through 11, for more information).

11. Develop and implement an IT contingency plan that meets USFR requirements and credible industry standards and test the plan at least annually to identify and remedy deficiencies and document the test results (see Finding 2, pages 6 through 11, for more information).

12. Develop and implement policies and procedures to oversee and routinely evaluate compliance with transportation laws and regulations for services provided through its transportation IGA, including verifying bus driver credentials, ensuring required drug testing is conducted, and confirming that buses and vehicles used to transport students meet Minimum Standards (see Finding 3, pages 12 and 13, for more information).

13. Develop and implement a process for routinely verifying the accuracy of student transportation counts and route mileage data provided by Patagonia UHSD before submitting reports to ADE to ensure accurate funding calculations (see Finding 3, pages 12 and 13, for more information).

14. Evaluate its transportation IGA to determine whether it fully addresses issues such as access to records for compliance reviews and whether changes are warranted to the amount the District pays for transportation services (see Finding 3, pages 12 and 13, for more information).

15. Develop and provide annual training to responsible District staff on transportation program requirements and oversight responsibilities (see Finding 3, pages 12 and 13, for more information).

APPENDIX

Objectives, scope, and methodology

We have conducted a performance audit of Sonoita Elementary School District on behalf of the Arizona Auditor General pursuant to A.R.S. §41-1279.03(A)(9). This audit focused on the District's efficiency and effectiveness primarily in fiscal year 2023, unless otherwise noted, in the 4 operational areas bulleted below because of their effect on instructional spending, as previously reported in the Arizona Auditor General's annual *Arizona School District Spending Analysis*. This audit was limited to reviewing instructional and noninstructional operational spending (see textbox). Instructional spending includes salaries and benefits for teachers, teachers' aides, and substitute teachers; instructional supplies and aids such as paper, pencils, textbooks, workbooks, and instructional software; instructional activities such as field trips, athletics, and co-curricular activities, such as choir or band; and tuition paid to out-of-State and private institutions.

Operational spending

Operational spending includes costs incurred for the District's day-to-day operations. It excludes costs associated with acquiring capital assets (such as purchasing or leasing land, buildings, and equipment), interest, and programs such as adult education and community service that are outside the scope of preschool through grade 12 education.

Noninstructional spending reviewed for this audit includes the following operational categories:

- **Administration**—Salaries and benefits for superintendents, principals, business managers, and clerical and other staff who perform accounting, payroll, purchasing, warehousing, printing, human resource activities, and administrative technology services; and other spending related to these services and the Governing Board.
- **Plant operations and maintenance**—Salaries, benefits, and other spending related to equipment repair, building maintenance, custodial services, groundskeeping, security, and spending for heating, cooling, lighting, and property insurance.
- **Food service**—Salaries, benefits, food supplies, and other spending related to preparing, transporting, and serving meals and snacks.
- **Transportation**—Salaries, benefits, and other spending related to maintaining school buses and transporting students to and from school and school activities.

Financial accounting data and internal controls—We evaluated the District's internal controls related to processing expenditures and scanned fiscal year 2023 payroll and accounts payable transactions in the District's detailed accounting data for proper account classification and reasonableness. Additionally, we reviewed detailed payroll and personnel records for 30 of 41 individuals who received payments through the District's payroll system in fiscal year 2023 and reviewed supporting documentation for 40 of 1,296 fiscal year 2023 accounts payable transactions. In addition, we reviewed fiscal year 2023 spending compared to the previous year and trends for the different operational categories to assess reasonableness and identify significant changes in spending patterns. We also evaluated other internal controls that we considered significant to the audit objectives. This work included reviewing the District's policies and procedures and, where applicable, testing compliance with these policies and procedures; reviewing controls over the District's network and information systems; and reviewing controls over reporting various information used for this audit. We reported our results on applicable internal control procedures in Finding 1 (see pages 3 through 5).

Peer groups—The Arizona Auditor General developed 3 types of peer groups for comparative purposes. To compare the District's student achievement, the Arizona Auditor General developed a peer group using poverty rates, district type, and location because these factors are associated with student achievement. We used this peer group to compare the District's fiscal year 2023 student passage rates on State assessments as reported by ADE. We also reported the District's fiscal year 2023 ADE-assigned school letter grade.

To compare the District's operational efficiency in administration, plant operations and maintenance, food service, and transportation, we used the Arizona Auditor General's peer groupings that are based on district size and location. They used these factors because they are associated with districts' cost measures in these areas. For very small districts, such as Sonoita ESD, increasing or decreasing student enrollment by just a few students or employing 1 additional part-time position can substantially impact the district's costs per student in any given year. As a result, and as noted in the *Arizona School District Spending Analysis—Fiscal year 2023,* very small districts' spending patterns are highly variable and result in less meaningful group averages. Therefore, in evaluating the efficiency of the District's operations, less weight was given to various cost measures, and more weight was given to our reviews and analysis of the District's operations.

Table 2: Criteria for selecting peer school districts for comparative purposes—Fiscal year 2023

Comparison areas	Factors	Group characteristics	Number of districts in peer group
Student achievement	Poverty rate District type Location	Less than 15% Elementary school districts Towns and rural areas	11
Administration, plant operations and maintenance, and food service	District size Location	Very small Towns and rural areas	58
Transportation	Location	Towns and rural areas	53

Source: Walker & Armstrong staff review of the Arizona Auditor General's *Arizona School District Spending Analysis–Fiscal year 2023*.

Efficiency and effectiveness—In addition to the considerations previously discussed, we also considered information from various sources that impact spending and operational efficiency and effectiveness as described below:

- **Interviews—**We interviewed various District employees about their duties in the operational areas we reviewed. This included District and school administrators, department supervisors, and other support staff who were involved in activities we considered significant to the audit objectives.

- **Observations—**To further evaluate District operations, we observed various day-to-day activities in the operational areas we reviewed. This included facility tours, food services operations, IT operations, and transportation services.

- **Report reviews—**We reviewed various summary reports of District-reported data including its *Annual Financial Report*, Single Audit reports, and USFR compliance questionnaire results that its external financial audit firm completed. We also reviewed District-provided accounting system and network user account reports. Additionally, we reviewed Department of Public Safety school bus inspection reports for the school buses inspected in calendar years 2021 through 2023.[7]

- **Documentation reviews—**We reviewed various documentation provided by the District related to its fiscal year 2023 operations and spending including: District policies and standard operating procedures; credit card statements and supporting documentation for purchases; cash receipts documentation and bank statements; cash disbursement supporting documentation; employment contracts and payroll records; Governing Board meeting minutes; Governing Board member and District employee conflict-of-interest disclosures; annual staff orientation training agenda and attendance log; the District's outsourced IT contract; and mileage logs for all district vehicles. Additionally, we reviewed documentation provided by Patagonia UHSD including: school bus driver files for 6 school bus drivers who transported District students in fiscal year 2023; school bus trip inspection checklists for selected weeks of fiscal year 2023; and fiscal year 2023 school bus maintenance logs.[7]

- **Analysis—**We reviewed and evaluated the District's fiscal year 2023 spending on administration, plant operations and maintenance, food service, and transportation and compared it to peer districts. We also compared the District's square footage per student, use of building space, and meals served per student to peer districts.

We selected our audit samples to provide sufficient evidence to support our findings, conclusions, and recommendations. Unless otherwise noted, the results of our testing using these samples were not intended to be projected to the entire population.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We express our appreciation to the District's Governing Board members, superintendent, and staff for their cooperation and assistance throughout the audit, as well as the Arizona Auditor General's Office for their support.

[7] The District has an agreement with Patagonia UHSD for transportation services, so our review of student transportation was performed for Patagonia UHSD school buses and bus drivers (see Finding 3, pages 12 and 13, for more information).

DISTRICT RESPONSE

Sonoita Elementary School District
Elgin School
23 Elgin Rd
Elgin, AZ 85611
(520) 455-5514 Fax (520) 455-5516
Daniel R. Erickson, Superintendent

August 18, 2025

Lisa S. Parke
Walker & Armstrong
1850 N. Central Ave., Suite 400
Phoenix, AZ. 85004

Dear Ms. Parke,

Sonoita Elementary School District #25 has received and carefully reviewed the Fiscal Year 2023 Performance Audit Report prepared by Walker & Armstrong. We accept the findings and recommendations outlined in the report. Of the 15 recommendations provided, several have already been implemented, and we are actively working to complete the remaining items.

Our District remains committed to delivering the highest quality education to our students in a safe and secure environment, maintaining an efficient and supportive workplace for our employees, and serving our constituents and community as responsible stewards of public funds. We will continue to work diligently to implement the audit recommendations and to remain current with compliance updates and future requirements.

We extend our sincere appreciation to Walker & Armstrong and their audit team for their thorough work and professional guidance throughout this process. Your team's expertise and support have been instrumental in strengthening the District's operations.

Sincerely,

Daniel R. Erickson
Superintendent/Principal
Sonoita Elementary School District #25
23 Elgin Rd., Elgin, AZ. 85611
520-455-5514

Finding 1: District lacked important internal controls over cash and some purchases and did not follow requirements in other areas, increasing the risk for errors, misuse, and fraud.

District Response: The finding is agreed to.

Recommendation 1: Develop and implement policies and procedures for cash receipts and disbursements that include: limiting access to the accounting system or implementing a review process to detect improper transactions or errors; reconciling deposits to cash receipts; requiring 2 individuals to open mail and prepare/sign a log of cash receipts; separating duties related to accounting system access, check signing, and bank reconciliations; and requiring dual authorization for bank transfers.

District Response: The audit recommendation will be implemented.

Response explanation: Upon being made aware of the deficiency, the District modified its policies and procedures to allow further separation of duties in business operations, cash reconciliations and mail receipt and handling.

Recommendation 2: Develop and implement policies and procedures to ensure that transactions made by its superintendent, including travel requests, are approved in advance, and ensure that the superintendent's credit card and travel expenses are specifically identified for final Board approval.

District Response: The audit recommendation will be implemented.

Response explanation: The District has implemented this recommendation after being notified of the deficiency.

Recommendation 3: Immediately terminate the employment of any Board member to comply with State law.

District Response: The audit recommendation will be implemented.

Response explanation: The District no longer employs Board members.

Recommendation 4: Provide additional training to Board members and staff on statutory conflict-of-interest requirements, including employment, disclosure, and recusal obligations, and document the training provided.

District Response: The audit recommendation will be implemented.

Response explanation: Subsequent to the audit the District implemented a policy and performed an in depth annual Board training on the recommended subject content.

Finding 2: District's excessive access to its sensitive computerized data and other IT deficiencies increased the risk of unauthorized access to its critical systems and sensitive information, errors, fraud, and data loss.

District Response: The finding is agreed to.

Recommendation 5: Require access controls restricting the ability of users to share, copy, or download documents, and to track and monitor cloud-based storage activity, and investigate any unusual activities that are identified.

District Response: The audit recommendation will be implemented.

Response explanation: Upon being notified of the data share, the District worked with our IT department, all access to external data sharing has been blocked. The District worked with the employee, IT department and the Superintendent to address the incident. The District reviewed data sharing policy/procedure with all staff at all staff meeting in Oct. 2024.

Recommendation 6: Assign and periodically review user access to the District's cloud-based storage, accounting information, and student information systems to ensure users have access to only those functions needed to perform their assigned duties. If separation of duties is not feasible due to limited staffing, the District should implement other controls such as a process for a supervisor to regularly review information such as transaction details, system logs, and activity reports, as required by the USFR.

District Response: The audit recommendation will be implemented.

Recommendation 7: Centrally manage user access and enforce security policies across all devices, including strong password requirements that align with credible industry standards.

District Response: The audit recommendation will be implemented.

Recommendation 8: Develop and provide training to users on IT security topics, such as password management, session timeouts, login attempt restrictions, and requirements to store all sensitive data on the District's approved cloud-based storage system; and document the training provided.

District Response: The audit recommendation will be implemented.

Recommendation 9: Immediately disable or remove all unnecessary user accounts in its cloud-based storage and student information systems and implement a review process to ensure access to all systems is removed immediately when an employee or vendor service is terminated.

District Response: The audit recommendation will be implemented.

Response explanation: Upon being notified of the deficiency, the District removes all access to systems upon termination.

Recommendation 10: Protect sensitive computerized systems and data by evaluating and implementing appropriate security measures for its wireless and internal network.

District Response: The audit recommendation will be implemented.

Recommendation 11: Develop and implement an IT contingency plan that meets USFR requirements and credible industry standards and test the plan at least annually to identify and remedy deficiencies and document the test results.

District Response: The audit recommendation will be implemented.

Finding 3: District did not oversee its outsourced transportation services, increasing the risk of student safety concerns, reporting errors, and fraud.

District Response: The finding is agreed to.

Recommendation 12: Develop and implement policies and procedures to oversee and routinely evaluate compliance with transportation laws and regulations for services provided through its transportation IGA, including verifying bus driver credentials, ensuring required drug testing is conducted, and confirming that buses and vehicles used to transport students meet Minimum Standards.

District Response: The audit recommendation will be implemented.

Recommendation 13: Develop and implement a process for routinely verifying the accuracy of student transportation counts and route mileage data provided by Patagonia UHSD before submitting reports to ADE to ensure accurate funding calculations.

District Response: The audit recommendation will be implemented.

Recommendation 14: Evaluate its transportation IGA to determine whether it fully addresses issues such as access to records for compliance reviews and whether changes are warranted to the amount the District pays for transportation services.

District Response: The audit recommendation will be implemented.

Recommendation 15: Develop and provide annual training to responsible District staff on transportation program requirements and oversight responsibilities.

District Response: The audit recommendation will be implemented.

Walker & Armstrong

CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS