



ARIZONA AUDITOR GENERAL

Lindsey A. Perry, Auditor General

Melanie M. Chesney, Deputy Auditor General

December 31, 2025

Members of the Arizona Legislature

The Honorable Katie Hobbs, Governor

Governing Board
Maine Consolidated School District

Justin Roberson, Superintendent
Maine Consolidated School District

Transmitted herewith is a report of the Auditor General, *A Performance Audit of Maine Consolidated 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 Roberson 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

Maine Consolidated School District

District's student assessment scores far exceeded peer and State averages, but the District lacked some internal controls related to cash handling and purchasing, and did not comply with IT security requirements, putting public monies and sensitive computerized data at risk

Performance Audit
A Report to the Arizona Legislature
December 2025
Report 25-215





CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

December 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 Maine Consolidated School District for fiscal year 2024, conducted pursuant to Arizona Revised Statutes §41-1279.03.

As outlined in its response, the District agrees with 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,

A handwritten signature in black ink that reads "Walker & Armstrong, LLP".

Walker & Armstrong, LLP
Phoenix, Arizona

Maine Consolidated School District

District's student assessment scores far exceeded peer and State averages, but the District lacked some internal controls related to cash handling and purchasing, and did not comply with IT security requirements, putting public monies and sensitive computerized data at risk

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 engaged in a complicated process for depositing cash receipts, increasing the risk for errors, loss, theft, and fraud.
- District did not separate responsibilities for purchasing and receiving goods and services and did not ensure that purchases were approved in advance, increasing the risk of unnecessary purchases, overspending, and/or fraud.
- District failed to implement critical information technology (IT) security requirements, such as aligning password requirements with credible industry standards, limiting user access to its network devices and accounting system, developing a complete IT contingency plan, and ensuring staff receive cybersecurity training to reduce the risk of unauthorized access, data loss, errors, and fraud.
- District operated outdated IT systems that were not receiving critical security updates, increasing the risk of data loss, cyberattacks, and disrupted operations.

Key recommendations

The District should:

- Develop and implement policies and procedures to separate cash-handling and reconciliation duties and responsibilities for purchasing and receiving goods and services.
- Comply with USFR requirements and District policy to deposit cash receipts intact and at least weekly, regardless of whether cash receipts are in the form of currency or checks.
- Ensure staff comply with District policies to obtain advance approval for purchases and ensure that purchase approval dates are documented.
- Develop and implement comprehensive IT procedures to establish and enforce strong password requirements, limit unnecessary user access to IT systems, establish and regularly test an IT contingency plan, and ensure all staff receive cybersecurity awareness training.
- Replace IT systems that no longer receive critical security updates.

TABLE OF CONTENTS

District overview	1
Finding 1	3
District did not follow requirements in some areas, potentially putting public monies at risk	
Deficiency 1: District did not comply with important cash-handling requirements, increasing the risk of errors, loss, theft, and fraud	
Deficiency 2: District did not comply with some USFR requirements for purchasing goods and services, increasing the risk of unnecessary purchases, overspending, and/or fraud	
Recommendations	
Finding 2	7
Numerous IT deficiencies, including unrestricted user permissions on network devices and outdated and unsupported systems, pose cybersecurity risks to District systems and critical data	
District has not complied with some important IT security requirements and credible industry standards	
Deficiency 1: District's authentication controls did not meet USFR requirements and credible industry standards	
Deficiency 2: District did not regularly review and restrict user permissions on network devices, provided too much access to its accounting system, and did not disable all unneeded accounts	
Deficiency 3: District lacked a complete IT contingency plan, increasing the risk of extended disruptions to operations	
Deficiency 4: District could not verify that all employees received annual cybersecurity awareness training	
Deficiency 5: Some District IT systems no longer receive critical security updates	
Recommendations	
Summary of recommendations	11
Walker & Armstrong makes 12 recommendations to the District	

Appendix

a-1

Objectives, scope, and methodology


District response

Tables

Table 1: Criteria for selecting peer school districts for comparative purposes—Fiscal year 2024

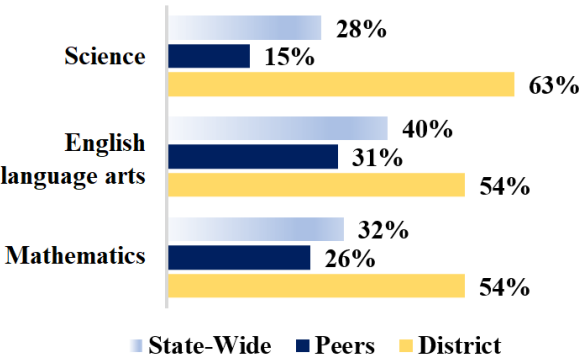
a-2

Maine Consolidated School District—Performance Audit
Fiscal Year 2024
December 2025



Rural district in Coconino County
Grades: Kindergarten through 8th
FY 2024
Students attending: 115
Number of schools: 1
School letter grade¹: A

Students who passed State assessments²



¹ Source: Arizona State Board of Education 2023-2024.
² Source: Arizona Auditor General’s *Arizona School District Spending Analysis—Fiscal year 2024 and data file*.

FY 2024 total operational spending – \$2.73 million (\$23,716 per student)	
Instructional – 54% (\$12,894 per student)	Noninstructional – 46% (\$10,822 per student)

Operational overview—FY 2024	Measure	Maine CSD	Peer average
Administration—lower per student spending, but improvements needed <p>The District spent substantially 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. For example, the District’s superintendent also acts as its principal. However, the District lacked internal controls over cash receipts and disbursements and did not comply with important IT standards, putting public monies and sensitive information at an increased risk of errors, fraud, and data loss (see Findings 1 and 2, pages 3 through 10).</p>	Spending per student	\$2,772	\$4,306
Plant operations—lower spending and no reported findings <p>The District spent less on plant operations than its peer districts averaged and has only 1 individual designated to maintain its facilities. This individual is also shared with the transportation department, permitting the District to allocate salary costs accordingly. We did not report any findings in this area.</p>	Spending per square foot	\$9.11	\$9.68
	Spending per student	\$2,339	\$3,197

Food service—higher spending and no reported findings The District spent more per meal and per student on food service than its peer districts averaged, likely because the District employs dedicated food service staff. In comparison, peer districts with similar student populations may assign food service responsibilities to administrative staff. We did not report any findings in this area.	Spending per meal	\$11.08	\$7.77
	Spending per student	\$1,170	\$1,141
Transportation—higher spending and no reported findings The District spent more per mile and rider on its transportation program than its peer districts averaged, likely due to higher salary and benefit costs resulting from the number of bus routes the District operates. Approximately 48% of the District’s students reside outside the District’s boundaries and the District operates several bus routes for these students to ensure timely student transportation. We did not report any findings in this area.	Spending per mile	\$6.89	\$3.19
	Spending per rider	\$4,646	\$2,058

District did not follow requirements in some areas, potentially putting public monies at risk

As part of our review, we identified issues relating to the District's failure to safeguard cash and comply with purchasing requirements, including verifying that it had received goods and services prior to making payments to vendors. See the details below.

Deficiency 1: District did not comply with important cash-handling requirements, increasing the risk of errors, loss, theft, and fraud

We found that the District did not comply with the *Uniform System of Financial Records for Arizona School Districts* (USFR) cash-handling requirements to ensure all public monies were properly safeguarded.¹ The USFR requires districts to implement policies and procedures that provide effective internal controls over cash receipts. These controls are intended to safeguard cash, prevent unauthorized transactions, and ensure financial transparency. Our review of the District's cash-handling policies and procedures found that some were not in accordance with USFR requirements and/or were not consistently followed. Specifically:

- Contrary to the USFR, the District did not separate most cash-handling responsibilities—**
 The USFR requires financial responsibilities to be separated to ensure proper oversight and reduce the risk of errors, loss, theft, and fraud, but District procedures specify that the business manager is responsible for performing most of the District's cash-handling functions. These responsibilities include preparing deposits and safeguarding cash, reconciling cash receipts to deposits, recording cash receipt transactions in the accounting system, and reconciling bank statements. Additionally, as further discussed in Finding 2, pages 7 through 10, the District improperly granted its business manager administrator-level access to the District's accounting system. This level of access gave the business manager the ability to requisition and approve purchases, add vendors to the system, and approve and pay invoices without another employee's review or approval.

Although we did not identify any improper transactions resulting from these deficiencies, this concentration of duties and excessive accounting system access gave the business manager the ability to manipulate financial records, misappropriate funds, or conceal errors without independent oversight. When we made the District aware of these issues during the audit, officials stated that they were unaware of these deficiencies and the associated risks and would work to develop appropriate controls to address the identified weaknesses.

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.

- **District staff did not restrictively endorse checks upon receipt, as required by the USFR—**The USFR requires that districts endorse checks received “for deposit only” to reduce the risk of fraud or misappropriation, but District staff did not do so and the District’s policies and procedures did not require it. We randomly selected and reviewed 31 of 542 fiscal year 2024 cash receipts and found that the District had not restrictively endorsed any of the checks we reviewed. The District reported that it deposits checks electronically and staff were unaware of any risks associated with checks that are not restrictively endorsed. However, by not restrictively endorsing checks upon receipt as required, the District increased the risk that any lost or stolen checks could be fraudulently cashed.
- **District’s business manager engaged in complicated process to make it appear as though cash was timely deposited, but the effort still resulted in untimely deposits and potentially increased the risk for fraud, errors, and loss—**The USFR and District policy require cash to be deposited at least weekly, or daily when amounts are significant, but we found that the District did not meet this and other requirements related to cash deposits. We randomly selected and reviewed 31 of 542 cash receipts recorded during fiscal year 2024 and found that the District had not deposited 4 receipts, totaling \$1,103, within the required timeframe. In addition, we reviewed the District’s fiscal years 2023 and 2024 USFR Compliance Questionnaires performed by the District’s independent financial auditors, which similarly found untimely deposits. Although the District electronically deposited checks it received, the District’s business manager indicated that the District had difficulty meeting the weekly deposit requirement for currency because the District is located approximately 38 miles roundtrip from its bank.

In a misguided attempt to address this deficiency, the business manager developed a complicated process she believed would make it appear as though the District’s deposits were timely. The business manager’s process involved using checks the District collected to represent currency amounts the District had collected for purposes of preparing deposits, and then depositing the collected currency at a later date. For example, on August 2 and 3, 2023, the District’s receipts indicated it collected a total of \$305—\$70 in currency and \$235 in checks. Rather than preparing the deposit for the \$305 amount, the business manager waited to prepare a deposit until the District received an additional \$70 in checks to match the \$70 in currency, which the District stored in a safe. Upon collecting the additional \$70 in checks, the business manager then electronically deposited \$305—all checks—on August 16, which was not within the 7 days required by the USFR. The \$70 in currency the District collected on August 2 and 3 was not deposited until the District transported the currency to its bank on August 25—15 days past the timeframe set by the District’s policy and the USFR.

The business manager’s complicated process not only failed to resolve the delayed deposits but also resulted in difficulty reconciling cash deposits to receipts and increased the risk of fraud, errors, and loss. Specifically, although the District issued prenumbered receipts for currency and cash received as required by the USFR, the business manager’s process made it such that cash collected and receipted on the same day was routinely separated among different bank deposits. This complicated process contains the elements of a lapping scheme, which is frequently used as a means of stealing cash and perpetrating fraud. Although we did not identify missing monies, we were unable to reconcile the District’s deposits with the receipts we reviewed without assistance from the business manager. Further, as previously discussed, the District did not

separate responsibilities for reconciling cash deposits and bank statements, but made the business manager responsible for nearly all cash-handling responsibilities, contrary to the USFR. By failing to separate cash-handling responsibilities and allowing the problematic cash deposit practice to continue, the District reduced accountability and increased the risk of fraud, errors, and loss.

Deficiency 2: District did not comply with some USFR requirements for purchasing goods and services, increasing the risk of unnecessary purchases, overspending, and/or fraud

The District did not comply with USFR purchasing requirements to ensure purchases were approved in advance and that all goods and services were received prior to processing payments. Specifically:

- **Not all purchases were approved in advance, and the District lacked documentation of the date when some purchases were approved**—The USFR and District policy require approval prior to purchasing goods and services, but the District did not consistently follow its policy and also lacked documentation to demonstrate when some purchases were approved. We randomly selected and reviewed 36 of 786 fiscal year 2024 expenditures and identified 1 instance where the District purchased 2 storage containers for \$7,972 without advanced approval. District staff were unable to explain why the purchase order was not approved prior to initiating the transaction but reported that the transaction may have received prior verbal approval and was an authorized purchase. Additionally, we found that approvals for purchases are performed directly in the accounting system and do not contain an approval date, therefore, we were unable to determine whether the purchases were approved in advance, as required.
- **The District's receiving processes do not comply with USFR requirements and purchasing responsibilities are not appropriately separated**—Contrary to the USFR, the District lacked documentation that all purchases were received, and it has not separated purchasing and receiving responsibilities among staff. Specifically, we found that the District did not document the receipt of 20 of 36 purchases we reviewed. The business manager reported reviewing the receipt of items delivered to the District's business office and confirming with other departments that they received goods or services delivered directly to those departments. However, the business manager did not use receiving reports or other means to document that goods or services were received and to provide support for payments, and there is no requirement to do so under District policy. Additionally, according to District policy, the business manager is responsible for verifying that items ordered were received and are in working order and for purchasing goods and services, which are duties that should be separated to reduce the risk of fraud.

By failing to comply with USFR requirements for purchasing and receiving, the District is at an increased risk for improper spending, fraud, and theft. Specifically, without advance approval, the District cannot ensure that all purchases are for valid District purposes and do not result in overspending. Additionally, the District's lack of a documented receiving process heightens the risk of paying for goods or services that were not received or do not meet quality standards, and of paying fraudulent invoices. Moreover, by not separating the responsibilities for purchasing and receiving, the District increases the risk of potentially fraudulent purchases and/or goods being misappropriated and

going undetected. After we brought these issues to the District's attention, the District reported that it would evaluate its policies and procedures and implement any necessary changes to better safeguard public monies.

Recommendations to the District

1. Develop and implement policies and procedures for cash handling that comply with USFR requirements, including separating cash-handling and bank reconciliation responsibilities, and restrictively endorsing checks immediately upon receipt as "for deposit only."
2. Comply with USFR requirements and District policy to deposit cash receipts intact and at least weekly, regardless of whether cash receipts are in the form of currency or checks.
3. Follow its policy to require an approved purchase order prior to purchasing goods or services, and ensure such approvals are dated.
4. Develop and implement purchasing policies and procedures that comply with USFR requirements, including requiring an individual independent of the purchasing process to verify and document the receipt of goods and services.

District response: As outlined in its [response](#), the District agrees with the finding and will implement the recommendations.

Numerous IT deficiencies, including unrestricted user permissions on network devices and outdated and unsupported systems, pose cybersecurity risks to District systems and critical data

District has not complied with some 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 and prevent errors, fraud, and data loss. 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, data loss, errors, and fraud. See the details below.

Deficiency 1: District's authentication controls did not meet USFR requirements and credible industry standards

As of May 2025, the District's password requirements for some critical systems did not meet USFR requirements to align with credible industry standards, such as those developed by NIST. As a result, the District increased the risk that unauthorized individuals could access sensitive District information and disrupt District operations. After we brought this issue to the District's attention, it began working with its IT system provider to address this deficiency.

Deficiency 2: District did not regularly review and restrict user permissions on network devices, provided too much access to its accounting system, and did not disable all unneeded accounts

Our May 2025 review of user accounts on the District's network, student information system (SIS), and accounting information system (AIS) found that the District did not limit users' access to network devices and a critical IT system in accordance with the USFR and credible industry standards. Additionally, it did not consistently disable user accounts that were no longer necessary. Specifically:

- **District permitted users to have local administrator access on their devices, contrary to recommended practices, and also improperly allowed 1 user too much access to its accounting system**—We found that 47 network users had local administrator access on their work computers and/or devices, which is more than what is necessary to perform their assigned duties and is counter to credible industry standards because of the associated security risk. Specifically, this level of access could enable users to intentionally or unintentionally download viruses, install unauthorized programs, or provide access to sensitive data or systems to unauthorized individuals.

We also found that the District had granted a user in the business office unnecessary administrator-level access to its accounting system. System administrator access allows the user to modify system settings and permissions, including adding, disabling, and changing access for all users. The administrator may also 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.

The District lacked a process for reviewing and assigning permissions and system access based on employees' job functions and responsibilities, and the District reported that prior to our review it was unaware of the access issues we identified. However, with regard to its accounting system, officials indicated that because of limited staffing they thought it was necessary for the business manager to have full access to the accounting functions. Similarly, as discussed in Finding 1, pages 3 through 6, the District had assigned the business manager conflicting responsibilities. When separating incompatible duties is not possible, the USFR requires school districts to implement additional management reviews or other compensating controls, such as regular supervisory reviews of transactions, system logs, and activity reports. Although we did not identify any improper transactions due to the business manager's conflicting responsibilities or excessive system access, the District has not developed a supervisory review process and assigned a supervisor or developed other compensating controls sufficient to effectively oversee those activities and mitigate the associated risks.

- **District did not disable unnecessary user accounts, increasing the risk of unauthorized and undetected use**—We identified 1 shared administrator account, previously used by the District's external IT provider, that was no longer needed because each IT administrator now operates under individual accounts. The continued existence of an unnecessary shared account, however, creates an unnecessary access point and increases the risk of unauthorized use or untraceable system activity.

Deficiency 3: District lacked a complete IT contingency plan, increasing the risk of extended disruptions to operations

Our May 2025 review of the District's contingency plan found that the plan lacked several components required by the USFR and recommended by credible industry standards to ensure continued operations, and the District had not tested the plan. Specifically, the District's plan did not include an assessment of potential risks and impacts, clear steps for when and how to activate the plan, or designate the individuals responsible for leading recovery efforts. The plan also lacked strategies for restoring operations, an inventory of critical systems and records, and a list of needed supplies. In addition, it did

not outline roles and communication procedures during a crisis or provide for regular updates and staff training on how to respond to emergencies. We also found that the District had not conducted required annual tests of its plan, which may have helped it to identify these deficiencies. By lacking a complete contingency plan and not testing its plan, the District increased the risk that it may not be able to effectively respond when systems go offline and may have extended disruptions to its operations.

Deficiency 4: District could not verify that all employees received annual cybersecurity awareness training

The USFR requires IT system users to receive basic annual security awareness training that addresses the prevention and detection of technology-related threats, but the District lacked documentation to support that it had trained all employees. Cybersecurity awareness training equips employees to recognize, avoid, and respond to common cyber risks, such as phishing, malware, and social engineering attacks and is a critical component in safeguarding the District's sensitive data and systems. We reviewed the District's sign-in log for fiscal year 2024 cybersecurity awareness training and found that approximately 10% of the District's employees did not sign the attendance roster. Although District officials stated that these employees completed the training at a later date, the District was unable to provide documentation supporting that all employees had completed the course as required.

Deficiency 5: Some District IT systems no longer receive critical security updates

Our May 2025 review found that the District was operating some IT systems that have exceeded their useful lifespans and may no longer receive critical security updates. The continued use of such systems is contrary to recommended practices and the USFR. According to the U.S. Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* and credible industry standards, districts should ensure that information systems are supported with current security updates to reduce the risk of vulnerabilities being exploited. The USFR also requires that districts implement security controls that protect the integrity, confidentiality, and availability of IT systems.

By using systems that do not receive regular security updates, the District increased its exposure to cybersecurity threats and disruptions to its operations. Specifically, the absence of vendor-supported patches may increase the likelihood of system vulnerabilities going unaddressed, which could affect the reliability and availability of critical IT services. District staff reported that budget limitations in prior years had necessitated the continued use of existing IT systems, but they were aware of the issue and were currently working to replace outdated equipment and software.

Recommendations to the District

5. Implement and enforce strong authentication controls that align with credible industry standards to decrease the risk of unauthorized persons gaining access to sensitive District information and disrupting operations.
6. Limit administrator-level access to devices on its network to only those individuals that the District determines need this level of access.

7. Limit employees' access to the accounting system to only those functions necessary to perform their job duties, including assigning administrator-level access to someone outside the business office. If separation of accounting and finance responsibilities is not feasible due to limited staffing, implement compensating controls such as additional supervisory reviews as required by the USFR.
8. Develop and implement written IT policies and procedures to specify user access levels by job function and responsibility and to conduct periodic reviews of user accounts to verify that access levels are appropriate.
9. Immediately disable or remove all unnecessary user accounts on its network and implement a formal review process to ensure access to its network and critical systems is promptly disabled or removed when no longer needed to reduce the risk of unauthorized access.
10. Develop an IT contingency plan that meets USFR requirements and credible industry standards and test the plan at least annually to identify and remedy deficiencies; document the test results.
11. Develop procedures to ensure that all District staff are provided with security awareness training at least annually and that such training is documented.
12. Replace IT systems that no longer receive critical security updates.

District response: As outlined in its [response](#), the District agrees with the finding and will implement the recommendations.

SUMMARY OF RECOMMENDATIONS

Walker & Armstrong makes 12 recommendations to the District

Recommendations to the District:

Finding 1

3

1. Develop and implement policies and procedures for cash-handling that comply with USFR requirements, including separating cash-handling and bank reconciliation responsibilities, and restrictively endorsing checks immediately upon receipt as “for deposit only.”
2. Comply with USFR requirements and District policy to deposit cash receipts intact and at least weekly, regardless of whether cash receipts are in the form of currency or checks.
3. Follow its policy to require an approved purchase order prior to purchasing goods or services, and ensure such approvals are dated.
4. Develop and implement purchasing policies and procedures that comply with USFR requirements, including requiring an individual independent of the purchasing process to verify and document the receipt of goods and services.

Finding 2

7

5. Implement and enforce strong authentication controls that align with credible industry standards to decrease the risk of unauthorized persons gaining access to sensitive District information and disrupting operations.
6. Limit administrator-level access to devices on its network to only those individuals that the District determines need this level of access.
7. Limit employees’ access to the accounting system to only those functions necessary to perform their job duties, including assigning administrator-level access to someone outside the business office. If separation of accounting and finance responsibilities is not feasible due to limited staffing, implement compensating controls such additional supervisory reviews as required by the USFR.
8. Develop and implement written IT policies and procedures to specify user access levels by job function and responsibility and to conduct periodic reviews of user accounts to verify that access levels are appropriate.
9. Immediately disable or remove all unnecessary user accounts on its network and implement a formal review process to ensure access to its network and critical systems is promptly disabled or removed when no longer needed to reduce the risk of unauthorized access.
10. Develop an IT contingency plan that meets USFR requirements and credible industry standards and test the plan at least annually to identify and remedy deficiencies; document the test results.

11. Develop procedures to ensure that all District staff are provided with security awareness training at least annually and that such training is documented.
12. Replace IT systems that no longer receive critical security updates.

Objectives, scope, and methodology

We have conducted a performance audit of Maine Consolidated 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 2024, 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.

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

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.

- **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 2024 payroll and accounts payable transactions in the District's detailed accounting data for proper account classification and reasonableness. We randomly selected and reviewed a sample of 31 of 542 fiscal year 2024 cash receipts and supporting documentation. We also reviewed detailed payroll and personnel records for 23 of 41 individuals who received payments through the District's payroll system in fiscal year 2024, and we reviewed supporting documentation for 36 of 786 fiscal year 2024 accounts payable transactions, including travel. In addition, we reviewed fiscal year 2024 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 Findings 1 and 2 (see pages 3 through 10).

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 2024 student passage rates on State assessments as reported by ADE. We also reported the District’s fiscal year 2024 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 Maine CSD, 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 2024*, 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 1: Criteria for selecting peer school districts for comparative purposes—Fiscal year 2024

Comparison areas	Factors	Group characteristics	Number of districts in peer group
Student achievement	Poverty rate District type Location	34% or higher Elementary school Towns and rural areas	14
Administration, plant operations and maintenance, and food service	District size Location	Very small Towns and rural areas	58
Transportation	Location	Towns and rural areas	54

Source: Walker & Armstrong staff review of the Arizona Auditor General’s *Arizona School District Spending Analysis—Fiscal year 2024*.

Efficiency and effectiveness—In addition to the considerations previously discussed, we also considered other information from various sources that impacts 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 2023 and 2024.
- **Documentation reviews**—We reviewed various documentation provided by the District including District policies and standard operating procedures; credit card statements and supporting documentation for fiscal year 2024 purchases; cash receipts documentation and bank statements for fiscal year 2024; cash disbursement supporting documentation for fiscal year 2024; fiscal year 2024 employment contracts and payroll records; Governing Board meeting minutes for fiscal year 2024; Governing Board member conflict-of-interest disclosures for fiscal years 2024 and 2025; District employee conflict-of-interest disclosure forms for fiscal years 2024 and 2025; security awareness training materials and attendance logs for fiscal year 2024; all school bus driver files for fiscal year 2024; and mileage logs for district vehicles.
- **Analysis**—We reviewed and evaluated the District’s fiscal year 2024 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.

DISTRICT RESPONSE



Home of the "Mustangs"

MAINE CONSOLIDATED SCHOOL #10

10 Spring Valley Road PO Box 50010 Parks, AZ 86018

Superintendent - Dr. Justin Roberson

(928) 635-2115 Fax (928) 635-5320

December 22, 2025

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

Dear Ms. Parke,

Maine Consolidated School District #10 has received and carefully reviewed the Fiscal Year 2024 Performance Audit Report prepared by Walker & Armstrong. We accept the findings and recommendations outlined in the report. Of the 12 recommendations provided, several have already been implemented, and we are actively working to complete the remaining items.

Maine Consolidated School District #10 remains committed to delivering the highest quality education to our students, as well as serving our community as responsible stewards of public funds. We will continue to work diligently to implement the audit recommendations provided and to remain current with compliance updates and future requirements.

We sincerely appreciate the audit team of Walker & Armstrong for their professional guidance throughout the process. Your team's expertise and assistance have been influential in strengthening our District's operations.

Sincerely,

Dr. Justin Roberson
Superintendent
Maine Consolidated School District #10
10 N. Spring Valley Rd., Parks, AZ. 86018
928-635-2115

Finding 1: District did not follow requirements in some areas, potentially putting public monies at risk.

District Response: The finding is agreed to.

Response explanation:

Recommendation 1: Develop and implement policies and procedures for cash handling that comply with USFR requirements, including separating cash-handling and bank reconciliation responsibilities, and restrictively endorsing checks immediately upon receipt as “for deposit only.”

District Response: The audit recommendation will be implemented.

Response explanation: District agrees to and has already implemented new procedures to comply with USFR requirements. We are endorsing checks immediately upon receipt as “for deposit only”

Recommendation 2: Comply with USFR requirements and District policy to deposit cash receipts intact and at least weekly, regardless of whether cash receipts are in the form of currency or checks.

District Response: The audit recommendation will be implemented.

Response explanation: The district will comply with USFR requirements as well as recommendations and District Policy, to deposit cash receipts intact and at least weekly, regardless of whether cash receipts are in the form of currency or checks.

Recommendation 3: Follow its policy to require an approved purchase order prior to purchasing goods or services, and ensure such approvals are dated.

District Response: The audit recommendation will be implemented.

Response explanation: The district will follow recommendation and policy to require an approved purchase order prior to purchasing goods or services, and ensure such approvals are signed and dated.

Recommendation 4: Develop and implement purchasing policies and procedures that comply with USFR requirements, including requiring an individual independent of the purchasing process to verify and document the receipt of goods and services.

District Response: The audit recommendation will be implemented.

Response explanation: The district has developed and implemented new procedures for checking in purchased goods to comply with USFR requirements which includes requiring an individual independent of the purchasing process to verify and document the receipt of goods.

Finding 2: Numerous IT deficiencies, including unrestricted user permissions on network devices and outdated and unsupported systems, pose cybersecurity risks to District systems and critical data.

District Response: The finding is agreed to.

Response explanation:

Recommendation 5: Implement and enforce strong authentication controls that align with credible industry standards to decrease the risk of unauthorized persons gaining access to sensitive District information and disrupting operations.

District Response: The audit recommendation will be implemented.

Response explanation: The district has implemented and will enforce strong authentication controls that align with credible industry standards to decrease the risk of unauthorized persons gaining access to sensitive District information and disrupting operations.

Recommendation 6: Limit administrator-level access to devices on its network to only those individuals that the District determines need this level of access.

District Response: The audit recommendation will be implemented.

Response explanation: The district will limit administrator-level access to devices on its network to only those individuals that the District determines need this level of access.

Recommendation 7: Limit employees' access to the accounting system to only those functions necessary to perform their job duties, including assigning administrator-level access to someone outside the business office. If separation of accounting and finance responsibilities is not feasible due to limited staffing, implement compensating controls such as additional supervisory reviews as required by the USFR.

District Response: The audit recommendation will be implemented.

Response explanation: Administrator has been added as a user for additional supervisory reviews as required by the USFR and access to other employees has been limited to job responsibilities.

Recommendation 8: Develop and implement written IT policies and procedures to specify user access levels by job function and responsibility and to conduct periodic reviews of user accounts to verify that access levels are appropriate.

District Response: The audit recommendation will be implemented.

Response explanation: The district will develop and implement written IT policies and procedures to specify user access levels by job function and responsibility and to conduct periodic reviews of user accounts to verify that access levels are appropriate.

Recommendation 9: Immediately disable or remove all unnecessary user accounts on its network and implement a formal review process to ensure access to its network and critical systems is promptly disabled or removed when no longer needed to reduce the risk of unauthorized access.

District Response: The audit recommendation will be implemented.

Response explanation: The district has removed all unnecessary user accounts on its network and will implement a formal review process to ensure access to the network and critical systems is properly disabled or removed when no longer needed to reduce the risk of unauthorized access.

Recommendation 10: Develop an IT contingency plan that meets USFR requirements and credible industry standards and test the plan at least annually to identify and remedy deficiencies; document the test results.

District Response: The audit recommendation will be implemented.

Response explanation: The district has developed an IT contingency plan that meets USFR requirements and credible industry standards and tests the plan at least annually to identify and remedy deficiencies; document the test results.

Recommendation 11: Develop procedures to ensure that all District staff are provided with security awareness training at least annually and that such training is documented.

District Response: The audit recommendation will be implemented.

Response explanation: The district has developed procedures to ensure that all District staff are provided with security awareness training at least annually and that such training is documented

Recommendation 12: Replace IT systems that no longer receive critical security updates.

District Response: The audit recommendation will be implemented.

Response explanation: The district has already replaced IT systems that can no longer receive critical security updates.

