ARIZONA Auditor General
Making a Positive Difference

Maine Consolidated School District

Initial Followup of Performance Audit Report 25-215

The December 2025 Maine Consolidated School District performance audit found that the District's student-assessment scores far exceeded peer and State averages. However, 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. The CPA firm Walker & Armstrong, LLP, which conducted the performance audit under contract with the Arizona Auditor General, made **12** recommendations to the District.

District's status in implementing 12 recommendations

Implementation status	Number of recommendations
Implemented	4 recommendations
In process	5 recommendations
Not implemented	**3 recommendations**

We will conduct a 24-month followup with the District on the status of the recommendations that have not yet been implemented.

Recommendations to the District

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

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."

- Status: **Implementation in process.**

  The District developed procedures to separate cash-handling responsibilities and restrictively endorse checks, as required by the *Uniform System of Financial Records for Arizona School Districts* (USFR).[1] However, the District could not demonstrate it had fully implemented its new procedures. We judgmentally selected and reviewed 81 cash receipts from April and May 2026 totaling $66,942 and found that the District did not consistently document who completed the various cash-handling steps. Specifically, we found that 32 cash receipts lacked documentation indicating who prepared the deposit, and 55 cash receipts lacked sufficient documentation to identify who deposited the cash at the bank. As such, we could not determine whether the District had separated its cash-handling responsibilities in accordance with USFR requirements, and the District continues to be at risk for loss, theft, or misuse. Additionally, although District officials reported that they were restrictively endorsing checks, we were unable to verify this because the District did not provide any evidence to support its assertion. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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.

- Status: **Implementation in process.**

  We reviewed all cash receipts and weekly deposits for April and May 2026 to determine whether the District followed its policy to deposit all cash receipts at least weekly. We identified 4 deposits that included approximately $4,000 in cash receipts that the District did not deposit within a week of collection. For the cash that was not deposited in accordance with the District's policy, District officials reported that staff had been unable to make the regularly scheduled deposit during the week the cash was collected. Consequently, District staff combined these monies with monies collected the following week and deposited them during their next regular trip to the bank.

  Since we completed our followup work, USFR guidance was updated to allow school district governing boards to establish an alternative regular deposit schedule when weekly deposits are not achievable or not financially advantageous. Given the District's

[1] The Arizona Auditor General and Arizona Department of Education jointly developed the USFR pursuant to Arizona Revised Statutes (A.R.S.) §15-271. The USFR and related guidance 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.

rural location and distance from its bank, the District's governing board may consider revising its policy for cash deposits to incorporate the USFR's updated guidance. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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

- Status: **Not implemented.**

  Contrary to District policy and USFR requirements, the District could not demonstrate that any of the 10 purchases made between January and June 2026 that we judgmentally selected for review had been properly approved prior to making the purchase.[2]

  Specifically:

  - 2 purchases lacked any evidence of a completed purchase requisition.
  - 1 purchase requisition lacked a required approval signature.
  - 7 purchase requisitions were signed by an authorized District official but lacked any information about when the approval occurred, such as a date on which the District official signed the requisition.

  District officials reported that they will ensure that future purchases are requested and approved in advance in accordance with the District's policies and the USFR. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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.

- Status: **Implementation in process.**

  Since the audit, the District revised its purchasing procedures to require an employee independent of the purchasing process to verify and document the receipt of any purchased goods prior to paying vendor invoices. However, the District's revised procedures are incomplete because they do not address how the District will verify that it has received purchased services prior to payment. Additionally, the District has not fully implemented its revised procedures. Specifically, we judgmentally selected and reviewed 10 purchases made between January and June 2026 and found that 6 purchases lacked evidence that the District had verified receipt of the purchased goods or services prior to the District paying the associated vendor invoices. District officials reported that they plan to improve the District's receiving process by November 2026. We will assess the District's efforts to implement this recommendation at the 24-month followup.

---

[2] The 10 purchases we reviewed totaled approximately $4,400 and included items such as school supplies, employee reimbursements, training, and sports-officiating services.

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

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.

- Status: **Implemented at 6 months.**

  Our July 2026 review of the District's IT authentication controls found that they aligned with credible industry standards.

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

- Status: **Implemented at 6 months.**

  The District limited administrator-level access on its network to only those individuals it determined had a need for this level of access. We reviewed all District network user accounts and found that none appeared to have unnecessary administrator-level access to the District's network.

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.

- Status: **Not implemented.**

  Although the District took some steps to address this recommendation, its efforts did not resolve the issues identified in the December 2025 performance audit and resulted in additional users having excessive accounting system access. District officials reported that they reviewed users' accounting system access levels and added additional office staff to better separate financial and accounting responsibilities. However, when assigning each user's system access, District officials did not ensure that no single user could complete a transaction without another employee's involvement. As a result, compared to the 1 user account with excessive system access identified during the performance audit, we found that 4 user accounts had more access than needed to perform their job duties and/or unnecessary administrator-level permissions. By continuing to allow some employees to have excessive accounting system access, the District is at risk for unauthorized transactions, unauthorized access to sensitive information, and fraud. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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.

- Status: **Not implemented.**

  The District has not developed written policies and procedures to guide staff responsible for reviewing and monitoring which accounting system functions each user has access to and whether any user has more access than necessary to perform their job duties. Although District officials reported that they review various system reports, such as change logs, this type of review acts as a compensating control to help identify improper system activity rather than as a check to ensure system access is appropriate. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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.

- Status: **Implementation in process.**

  The District has developed formal processes for ensuring that unnecessary user accounts are promptly removed and/or disabled and for conducting quarterly reviews of student and staff user accounts. However, the District's new review process does not consider vendor accounts. Our July 2026 review found that the unnecessary shared third-party IT administrator account identified in the December 2025 performance audit had not been disabled, as recommended. We followed up with the District's third-party IT provider, which reported disabling the account in September 2026. District officials reported that they will update the user account review process to include vendor accounts by November 2026. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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.

- Status: **Implementation in process.**

  The District created an IT contingency plan in July 2025, but the plan does not fully meet USFR requirements and credible industry standards. Specifically, the plan does not identify the IT systems critical to the District's operations, the order in which they should be restored, and who is responsible for carrying out disaster recovery duties. The plan also does not address how the District will continue to operate during an IT system outage. Additionally, the USFR requires school districts to test their contingency plans at least annually, and document any identified deficiencies and changes. We found that although the District had tested its system for data backup, it had not tested whether it could restore critical IT systems in accordance with its plan. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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

- Status: **Implemented at 6 months.**

  The District reported providing annual cybersecurity awareness training to all staff during summer in-service training sessions and requiring staff who start work after the beginning of the school year to complete the training within 30 days of hire. We reviewed the District's cybersecurity training completion log and confirmed that all current employees completed security awareness training in August 2026.

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

- Status: **Implemented at 6 months.**

  The District purchased new IT equipment in September 2025. District officials reported that the newly purchased equipment replaced systems identified during the audit that were no longer capable of receiving critical security updates.