




Mammoth-San Manuel Unified School District

Initial Followup of Performance Audit Report 24-213

The December 2024 Mammoth-San Manuel Unified School District performance audit found that the District spent less than peer districts on administration, but lacked some required internal controls and did not comply with important IT security requirements, putting student safety, District property, and sensitive computerized data at risk. The consulting firm Walker & Armstrong, who conducted the performance audit under contract with the Arizona Auditor General, made **9** recommendations to the District.

District's status in implementing 9 recommendations

Implementation status	Number of recommendations
 Implemented	3 recommendations
 In process	3 recommendations
 Not implemented	3 recommendations

We will conduct an 18-month followup with the District on the status of the recommendations that have not yet been implemented.

Recommendations to the District

Finding 1: District lacked important internal controls in some areas, potentially increasing the risk to student safety and District property

1. The District should review personnel files for employees who are required to have background checks to ensure that all required checks have been completed and documented.

▶ Status: **Not implemented.**

District officials indicated that since the audit, they had not reviewed personnel files to identify the employees who lacked documented background checks nor conducted background checks for these employees, as recommended. District officials indicated they did not do so because they believed they had conducted the required background checks and stored the results in a separate file, which they have been unable to locate. By continuing to lack documentation of required background checks demonstrating employees are qualified to work with students, the District has continued to potentially increase risks to student safety. We will assess the District's efforts to implement this recommendation at the 18-month followup.

2. The District should follow its process to complete an onboarding checklist for all newly hired employees.

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

District staff are required to complete a new-hire checklist for all newly hired District employees. Our review of personnel files for 5 District employees hired in calendar year 2025 found that each file contained a completed checklist, a completed Form I-9, and where required, a completed background check.

3. The District should develop and implement policies and procedures for training employees on required hiring documentation and document-retention time frames to comply with federal law and the USFR.

▶ Status: **Not implemented.**

District officials indicated they have not developed and implemented policies and procedures for training employees on required hiring documentation and document-retention time frames. Our September 2025 review of personnel files for 12 of 121 District employees found that 1 file did not contain a completed Form I-9 and 1 file did not contain a required background check, indicating that the recommended training continues to be important for ensuring the District complies with federal laws and the USFR. We will assess the District's efforts to implement this recommendation at the 18-month followup.

4. The District should retain documentation in personnel files in accordance with applicable document-retention schedules.

▶ Status: **Implementation in process.**

District officials indicated that they have provided document-retention guidance from Arizona State Library, Archives, and Public Records to staff and that staff meet annually to determine which personnel documentation should be destroyed. However, as noted in recommendation 3, we identified personnel files that lacked some required documentation, and therefore, additional work is needed to implement this recommendation. We will assess the District's efforts to implement this recommendation at the 18-month followup.

5. The District should develop and implement policies and procedures for monitoring and reviewing usage logs for all District vehicles that includes ensuring vehicles are used only for an authorized purpose.

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

According to District officials, all staff using a District vehicle are required to complete usage logs after each trip, including the driver, date of use, beginning and ending mileage, and purpose for using the vehicle. Additionally, they reported that the transportation supervisor reviews these logs monthly to ensure vehicles are used for authorized purposes. We reviewed usage logs from July to September 2025 for 5 of the District's 13 vehicles and found that District staff consistently filled out usage logs with all required information and the District conducted monthly reviews of the usage logs.

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

6. The District should protect its sensitive computerized data by limiting users' access to its accounting system and student information system to only those functions needed to perform their job duties, including removing the outside consultant's administrator-level access and business office employees' full access.

▶ Status: **Implementation in process.**

The District has taken some steps to reduce its users' excessive system access and no longer has any student information system users with more system access than necessary. However, as of September 2025, the District continued to allow excessive access to its accounting system. Specifically, 4 accounting system users continued to have excessive system access, including 1 user who could initiate and complete both purchasing and payroll transactions, and 3 users who could initiate and complete purchasing transactions. By continuing to allow excessive accounting system access, the District increases the risk of improper and fraudulent transactions. We will assess the District's efforts to implement this recommendation at the 18-month followup.

7. The District should develop and implement written policies and procedures to assign and periodically review accounting system access for employee accounts to ensure they have access to only those accounting system functions needed to perform their job duties. If separation of duties is not feasible due to a limited number of personnel, the District should implement other controls, such as a process for a supervisor to regularly review system logs, balancing reports, and other relevant indicators, as required by the USFR.

▶ Status: **Not implemented.**

The District has not yet developed written policies or procedures to guide staff responsible for assigning accounting system user access nor for conducting periodic reviews of user-access levels. Further, as discussed in recommendation 6, the District continues to allow some accounting system users to have excessive system access. District officials indicated they planned to create a list documenting appropriate access levels by position and would update access levels accordingly. We will assess the District's efforts to implement this recommendation at the 18-month followup.

8. The District should immediately disable or remove all unnecessary user accounts in its network and implement a review process to ensure network access is removed immediately when an employee or vendor relationship is terminated.

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

Since the audit, the District implemented a process to remove network access when an employee or vendor relationship is terminated. Our September 2025 review of the District's network user accounts did not identify any user accounts belonging to terminated employees or vendors who no longer worked for the District.

9. The District should develop and implement an IT contingency plan that meets USFR requirements and credible industry standards, test the plan at least annually to identify and remedy deficiencies, and document the test results.

▶ Status: **Implementation in process.**

The District developed an IT contingency plan and relevant staff reviewed the plan and acknowledged their respective roles in July 2025. However, the plan does not include all the information required by the USFR and recommended by credible industry standards, such as identifying all critical systems and the order in which those critical systems are to be restored. Additionally, although the plan states it should be periodically tested and District officials reported testing the plan, they did not document the test results. We will assess the District's efforts to implement this recommendation at the 18-month followup.