Report Highlights

Walker & Armstrong
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

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 compete 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- District operated outdated IT systems that were not receiving critical security updates, increasing the risk of data loss, cyberattacks, and disrupted operations.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.