East Ramapo Central School District
Report on Information Technology
For the Period July 1, 2023 through March 31, 2025

TABLE OF CONTENTS

Executive Summary	1
Overview, Procedures Performed, Observations, and Recommendations	2 – 6
Corrective Action Plan	6

R.S. ABRAMS & CO., LLP
Accountants & Consultants for Over 75 years

Robert S. Abrams
(1926-2014)

Marianne E. Van Duyne, CPA
Alexandria M. Battaglia, CPA
Brendan Nelson, CPA
Christopher Schneider, CPA

Board of Education
East Ramapo Central School District
105 South Madison Avenue
Spring Valley, New York 10977

We have been engaged by the Board of Education (the "Board") to provide internal audit services to East Ramapo Central School District (the "District") with respect to the internal controls related to information technology for the period July 1, 2023 through March 31, 2025.

The objectives of the engagement were to evaluate the efficiency, effectiveness, and compliance of the District's internal controls related to information technology with relevant policies, procedures, and regulatory requirements, where applicable.

Our procedures were not designed to express an opinion on internal controls related to information technology, and as such, we do not express such an opinion. Our audit of the District's information technology program identified areas of strength as well as opportunities for improvement. By implementing the recommended improvements, the District can further enhance the efficiency and effectiveness of its information technology program. The results of our procedures are presented on the following pages.

This report is intended solely for the information and use of the Board, the Audit Committee, and management of the District and is not intended to be and should not be used by anyone other than those specified parties.

We would like to acknowledge the courtesy and assistance extended to us by personnel of the District.

We are available to discuss this report with the Board or others within the District at your convenience.

Our observations and recommendations are directed at the improvement of the system of internal controls and should not be considered a criticism of, or reflection on, any employee of the District.

Very truly yours,

R. S. Abrams + Co., LLP

R.S. Abrams & Co., LLP
March 31, 2025

OVERVIEW, PROCEDURES PERFORMED, OBSERVATIONS, AND RECOMMENDATIONS

AREA: INFORMATION TECHNOLOGY (IT) POLICIES AND GOVERNANCE

Overview: School districts are legally required to implement information technology (IT) policies that ensure data privacy, cybersecurity, and compliance with state and federal regulations. Key policies include data privacy, security breach, and notification policy, Parent's Bill of Rights, and an acceptable use policy for internet and technology use. Policies must cover data breach notification, disaster recovery, network access controls, and security measures to protect student and staff information. These policies are regularly reviewed, updated, and made publicly available.

Relevant Board Policies Examined:

- Policy #8635, *Information and Data Privacy, Security Breach and Notification*
- Policy #8630, *Computer Resources and Data Management*
- Policy #8630-R, *Computer Resources and Data Management Regulations*

Procedures Performed:

- Conducted interviews with key District personnel to assess the IT governance framework, policy development, and risk management practices.
- Reviewed published Board policies for compliance with state and federal data privacy and cybersecurity regulations.
- Reviewed the Parent's Bill of Rights as published on the District's website to ensure compliance with FERPA (Family Educational Rights and Privacy Act).
- Verified the District engaged an IT specialist to perform penetration testing on the District's network noting the final report was issued on January 27, 2025.
- Reviewed ten IT vendor contracts to confirm that agreements include:
    - Data security and privacy provisions.
    - Signed copies of the Parent's Bill of Rights.
    - Confidentiality agreements covering student, teacher, and administrator data.

Observation: No exceptions noted.

Recommendation: No recommendations noted.

***

AREA: NETWORK SECURITY CONTROLS

Overview: The network security controls are designed to protect student, staff, and administrative data while ensuring compliance with state and federal regulations. Key security measures include firewalls, intrusion prevention systems (IPS), multi-factor authentication (MFA), and content filtering to safeguard against cyber threats and unauthorized access.

The District has implemented role-based access controls to limit system access based on job roles, ensuring users have appropriate permissions. The District secures Wi-Fi networks with WPA2/WPA3 encryption and network segmentation are in place to separate student, staff, and administrative traffic. Security monitoring tools are in place to detect and respond to threats. Additionally, the District continuously monitors network activity for anomalies and conducts vulnerability assessments and penetration tests to identify and mitigate potential risks.

Employees receive annual cybersecurity training, including phishing simulations and Safe Schools online training, to educate them on identifying, responding to, and reporting cyber threats.

Procedures Performed:

- Reviewed the District's policies and procedures regarding network and network access.
- Inquired with key District personnel to obtain an understanding of the network and network access procedures.
- Examined cybersecurity training material provided to employees to ensure significant topics and risks were discussed.
- Verified the District's network firewall is operational, regularly reviewed, and configured to block unauthorized access.
- Verified the District regularly performed updates and security patches to servers, workstations, and network devices.
- Verified remote access to the District systems are secured by multi-factor authentication.
- Verified physical controls such as access restrictions, temperature controls, fire suppression systems, and extinguisher placement in the District's server rooms exist and are operational.
- Sampled twenty (20) active users to confirm each employee completed mandatory cybersecurity training.

Observation: No exceptions noted.

Recommendation: No recommendations noted.

***

AREA: USER ACCESS CONTROLS

Overview: Employees are assigned role-based access controls based on the job responsibilities and duties. The District reviews user account permissions to ensure inactive or terminated employees are removed from the system timely. Each user has their own set of login credentials secured by password in accordance with District policy.

Procedures Performed:

- Verified user account administrative privileges are restricted to IT personnel and management.
- Reviewed polices and procedures included in the *Incident Response Plan* adopted on October 28, 2022 and revised on February 19, 2025.
- Reviewed active user accounts in the District's accounting information system to identify if duplicate or generic user accounts, and to ensure individual accounts are associated with only active District employees.
- Assessed whether automated alerts are in place to notify IT personnel of suspicious login activity (e.g., logins from unknown devices or unusual locations).
- Assessed whether system logs are reviewed to determine if unauthorized login attempts were detected.
- Sampled twenty (20) employees recently separated from the District to confirm the timely removal of their accounts from the accounting information system.

Observation: We reviewed the list of recently separated employees between 2023 and 2025 and identified 331 employees. Our analysis revealed the following:

- 36 out of 331 (11%) employees listed were marked as payroll active.
- 9 out of 331 (3%) employees listed as both human resources (HR) and payroll active.

To validate these findings, we compared the list of separated employees against the District's active user records. Our review confirmed that all nine employees identified as active in both the payroll and HR systems also had active user accounts. Upon consultation with the District, we determined that five of the nine employees remained employed in a reduced capacity. The remaining four employees were subsequently deactivated from the system.

Recommendation: We recommend that the District conduct a comprehensive review of separated employees to ensure proper deactivation of system access and payroll status.

***

AREA: BACKUP AND DISASTER RECOVERY

Overview: Backup and disaster recovery are designed to ensure the availability and integrity of critical IT systems and data in the event of a cyberattack, system failure, or natural disaster. The District maintains regular data backups, stored in a secure cloud environment, with encryption applied to protect sensitive student and staff information

Procedures Performed:

- Reviewed published Board policies to ensure the District's process is documented, conform with District policies, as well as applicable regulatory requirements, and accurately reflect the current operations of the District.
- Verified the District conducts nightly back-ups for critical systems and data.
- Reviewed the disaster recovery plan to verify
    - The plan aligns with NYSED and Education Law 2-d requirements
    - Roles and responsibilities are assigned for disaster recovery

  - Backup location, frequency and procedures are outlined in the plan
  - The plan is tested annually to verify the integrity of the plan.
  - Communication channels exist to communicate internally and externally.
- Verified the District performs recovery tests periodically during the year by reviewing the restore log noting a restore test is performed monthly.
- Verified the disaster recovery plan is updated and reviewed to reflect current operations of the District.

Observation: No exceptions noted.

Recommendation: No recommendations noted.

***

AREA: IT ASSET MANAGEMENT

Overview: The District's IT department maintains an inventory excel spreadsheet to track IT assets from procurement to disposal of IT equipment. The spreadsheet contains columns for the name, model and serial number.

Procedures Performed:

- Reviewed the IT asset inventory listing as of March 17, 2025 to assess accuracy, completeness, and proper classification of assets.
- Verified whether the District encrypted sensitive data on servers, individual computers, and portable devices.

Observation: The IT asset inventory listing does not include key information such as purchase date and cost. In addition, the District should consider adding ownership, location, asset status (active, retired, in repair, or decommissioned), disposal date, and warranty, if applicable.

Recommendation: We recommend the District perform a full IT inventory audit to expand information on the inventory listing to include purchase date and cost. In addition, we recommend the District consider adding ownership, location, asset status (active, retired, in repair, or decommissioned), disposal date, and warranty, if applicable.

***

AREA: INCIDENT RESPONSE AND CYBERSECURITY MONITORING

Overview: The District has an Incident Response Plan (IRP) that outlines procedures for identifying, containing, and mitigating cybersecurity incidents, such as data breaches, ransomware attacks, and unauthorized access. Automated cybersecurity monitoring tools, including intrusion detection systems (IDS), firewalls, and security logs, help detect and respond to threats in real time. IT staff receive alerts for suspicious activities.

Procedures Performed:

- Reviewed published Board policies to ensure the District's process is documented, conform with District policies, as well as applicable regulatory requirements, and accurately reflect the current operations of the District.
- Reviewed the IRP to verify:
  - Roles and responsibilities are clearly defined in the plan
  - The plan includes assessment steps for evaluating the severity of an incident
  - The plan includes clear steps for responding to incidents
  - A cybersecurity incident log is retained to track events.
- Verified whether the District retains a log of cybersecurity incidents and periodically reviews the log to identify potential trends.
- Reviewed the results of December 18, 2024 phishing simulation conducted noting no employee failed the simulation.

Observation: No exceptions noted.

Recommendation: No recommendations noted.

***

CORRECTIVE ACTION PLAN

The District is required to prepare a corrective action plan in response to any observations contained in the internal audit reports. As per Commissioner's Regulations §170.12, a corrective action plan, which has been approved by the Board, should be submitted to the State Education Department within 90 days of the receipt of a final internal audit report.

The approved corrective action plan and a copy of the respective internal audit report should be submitted using the NYSED Business Portal.