REPORT OF EXAMINATION | 2022M-68

East Bloomfield Central School District

Network and Financial Software Access Controls

SEPTEMBER 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

East Bloomfield Central School District

Audit Objective

Determine whether East Bloomfield Central School District (District) officials ensured network and financial software access controls were adequate to protect District information technology (IT) systems and data.

Key Findings

District officials did not ensure that network and financial software access controls were adequate to protect District IT systems and data from unauthorized access or loss. Sensitive network and financial software access control weaknesses were communicated confidentially to officials. In addition:

- The District had 250 unneeded network user accounts, including two with administrative permissions, and the Assistant Superintendent for Business and Operations had excessive administrative permissions in the financial software, which allowed them to potentially control all phases of financial transactions.
- Officials paid BOCES $539,644 for IT services in 2020-21 without defining roles and responsibilities for services. As a result, the roles and responsibilities of each party may not be understood by all parties resulting in cybersecurity gaps.

Key Recommendations

- Ensure officials enforce compliance with the data, network and security access policy.
- Disable unneeded network and financial software user accounts in a timely manner, and regularly review user accounts for necessity and appropriateness.
- Set written expectations for the District's specific IT service needs.

District officials agreed with our recommendations and indicated they will initiate corrective action.

Background

The District serves the Towns of Bristol, Canandaigua, East Bloomfield, Richmond, Victor and West Bloomfield in Ontario County.

The District is governed by a seven-member Board of Education (Board) that is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible for District administration.

The District's IT Director is responsible for managing IT operations, including network access controls, with assistance from two computer services assistants and Wayne-Finger Lakes Board of Cooperative Educational Services (WFL BOCES) staff.

The Assistant Superintendent for Business and Operations (Assistant Superintendent) manages user accounts and permissions for the financial software.

Quick Facts

Enabled Network User Accounts	
Student	1,218
Individual Non-Student	174
Service	10
Shared	26
Total	1,428
Financial Software	
Enabled User Accounts	50

Audit Period

July 1, 2020 – March 3, 2022

Network and Financial Software Access Controls

The District relies on its network and financial software for maintaining financial, student and personnel records, much of which contain personal, private and sensitive information (PPSI); accessing the Internet; and sending and receiving email. PPSI is any information to which unauthorized access, disclosure, modification, destruction, or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

If the District's network or financial software access is compromised or disrupted, the results could range from inconvenience to significant damage and could require extensive effort and resources to evaluate, repair and/or rebuild. While effective network and financial software access controls will not guarantee the safety of these systems, without these controls the District has an increased risk that its hardware, software and data, including PPSI, may be exposed, damaged or lost through inappropriate use, access and loss.

How Can Officials Establish Adequate Network and Financial Software Access Controls?

By adopting written policies and procedures, a school district board (board) can help ensure that officials establish adequate network and financial software access controls. Network and financial software access control policies should describe the tools to use and procedures to follow to help protect these systems and the data they contain, define appropriate user behavior when accessing the network and financial software and explain the consequences of policy violations.

A board should adopt policies that address topics including but not limited to user accounts, passwords, remote access (when a user is allowed to access the network or financial software from an off-site location) and audit trails (a record of activity that includes who has accessed the network or financial software, the time and date of the access and what activity occurred). A board also should ensure that officials monitor and enforce the policies and develop any required procedures to supplement the policies.

Without comprehensive written policies and procedures that explicitly convey a school district's network and financial software access controls, officials cannot ensure users are aware of their responsibilities for helping to protect these systems and the data they contain from unauthorized use, access and loss.

Officials Did Not Develop or Enforce Adequate Network and Financial Software Access Control Policies and Procedures

The Board adopted a written data, network and security access policy, but did not ensure that officials enforced compliance with the policy's requirements. The policy required the Superintendent (or their designee) to manage (i.e., grant,

change and terminate) user access rights and permissions for the network and specific software applications; develop password standards; authorize, monitor and control remote access; and establish procedures for periodically reviewing the network's audit trail.

District officials did not establish certain procedures as required by the policy. Without these procedures, the policy did not adequately address these areas. The IT Director told us that they were working on developing written procedures but were delayed by the COVID-19 pandemic and having a small technology staff.

We found that officials did not:

- Adequately manage user accounts for the network or financial software, including establishing adequate written procedures to add or disable user accounts or change user permissions. The IT Director developed limited informal procedures for adding and removing employee network user accounts in September 2021. However, the procedures were not adequately detailed, did not include guidance for network user permissions and did not address nonemployee network user accounts. Furthermore, officials did not develop procedures for financial software user access management.
- Develop written standards for network or financial software password security.
- Develop written procedures for adequately authorizing, monitoring and controlling remote access.
- Establish written procedures for reviewing audit trails and did not review network audit trail activity.

While network and financial software access control policies and procedures do not guarantee the safety of these District systems or the electronic information contained therein, without these policies and procedures the District has an increased risk that its hardware, software and data, including PPSI, may be exposed, damaged or lost through inappropriate access and use. Also, when officials do not regularly review network audit trails, they may not detect unauthorized or inappropriate activity within the network in a timely manner.

How Should Officials Manage Network and Financial Software User Account Access?

School district officials are responsible for restricting network user account access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and IT assets on the network are secure from unauthorized use, modification and/or loss.

Network and financial software user accounts provide access to network resources and financial and employee data and should be actively managed to minimize the risk of unauthorized access and misuse. If not properly managed, unneeded user accounts may not be detected and disabled in a timely manner. Also, unneeded accounts could be entry points for attackers to potentially access and view PPSI inappropriately, make unauthorized changes to records or deny legitimate access to electronic information when needed.

To minimize the risk of unauthorized access, misuse and loss, officials should actively manage network and financial software user accounts and permissions – including their creation, use and dormancy – and regularly monitor them to ensure they are appropriate and authorized. Officials should disable unneeded user accounts as soon as there is no longer a need for them.

A service account is an account created for the sole purpose of running a particular network or system service or application. Service accounts should be limited in use as they are not linked to individual users and, therefore, may have reduced accountability. For example, service accounts may be created and used for automated processes such as backups. Officials should limit the use of service accounts, routinely evaluate the need for them and disable those that are not related to a current school district or system need.

Shared user accounts are accounts with a username and password that are shared among two or more users. Shared accounts are often used to provide access to guests and other temporary or intermittent users (e.g., substitute teachers and third-party vendors). Because shared accounts are not assigned to an individual user, officials may have difficulty managing them and linking any suspicious activity to a specific user. Therefore, officials should limit the use of shared user accounts.

To help ensure individual accountability, each user should have and use their own user account, when possible. When shared user accounts are provided for temporary work or guests, the accounts should have an expiration date and automatically terminate access after a designated, authorized time period.

Generally, a network administrative account has user permissions to monitor and control a network, connected computers and certain applications, such as adding new users and changing user passwords and permissions. Additionally, a user with administrative permissions on a network can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. As a result, officials should limit network administrative permissions to those users who need them to complete their job duties and functions.

When financial software is used to process transactions and maintain financial records, adequate controls over access rights should allow users to access only

those functions that are consistent with their job duties and responsibilities. These controls also should prevent users from being involved in multiple phases of financial transactions.

The financial software administrator should not be involved in financial operations because an individual who has administrative rights to the software can generally add new users, configure software settings, override management controls, change user access rights, and record and adjust financial transactions.

Officials Did Not Adequately Manage Network and Financial Software User Account Access

District officials did not adequately manage network or financial software user account access. As a result, the District had unneeded, unused and shared user accounts and accounts with excessive user permissions that were not disabled or monitored.

We examined all 1,428 enabled network user accounts (1,218 student accounts, 174 individual nonstudent accounts, 10 service accounts and 26 shared accounts) and all 50 enabled financial software user accounts to determine whether accounts were necessary and appropriate.

Unneeded Individual Network User Accounts – Upon our request, District officials reviewed the 965 individual network user accounts (945 student accounts and 20 individual nonstudent accounts) that had not been used in at least six months. As a result, officials disabled 239 of the 965 accounts (25 percent), and three other individual user accounts that had been used in the past six months, because they were no longer needed. The disabled accounts included 236 former students who had graduated and five former employees, BOCES staff or others who were no longer employed or working at the District.

These accounts should have been disabled as soon as the individuals graduated, left District employment or stopped providing services to the District. Generally, these accounts were still enabled because IT staff did not have adequate procedures to follow for disabling accounts. Also, the IT Director told us that the staff member who was in charge of disabling student accounts recently retired, and the District did not have a process to identify when BOCES or other nonemployees stopped providing services to the District.

The IT Director determined that the remaining 726 inactive user accounts (709 students and 17 individual nonstudent accounts) were needed. The IT Director told us that these accounts were generally for students and staff who usually did not access the network, but should have accounts to do so if needed.

Unneeded Service and Shared Network User Accounts – There were 26 shared and 10 service network user accounts. Upon our request, District officials

reviewed the 13 shared and five service network user accounts that had not been used in the last six months. They told us that they disabled seven shared user accounts and one service network user account.

Of the seven accounts, six were shared accounts used by IT staff for software updates or as test accounts, which they plan to re-enable on an as-needed basis. Also, two of these disabled accounts had administrative permissions. The IT Director had not previously considered disabling certain accounts and enabling them only when needed.

In total, officials disabled 250 (18 percent) of the 1,428 enabled network user accounts, including two with administrative permissions. Unneeded user accounts are additional entry points into a network and, if accessed by an attacker, possibly could be used to inappropriately access and view PPSI.

When network user accounts are not used or monitored, compromised accounts may not be detected in a timely manner. In addition, when unneeded user accounts have administrative permissions, the District's risk compounds because the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

When network user accounts are not used or monitored, compromised accounts may not be detected in a timely manner.

Inappropriate Financial Software Permissions – We reviewed a sample of financial software permissions[1] for all 50 financial software user accounts to determine whether they were appropriate. We found that permissions were generally appropriate for financial software users with the exception of two accounts used by the Assistant Superintendent.

The Assistant Superintendent's two user accounts included one unique individual account and another account with administrative permissions. Both of these accounts had excessive user permissions that the Assistant Superintendent did not need to perform their job duties. District officials inappropriately designated the Assistant Superintendent as a financial software administrator even though the Assistant Superintendent was not independent of financial transactions. Therefore, the Assistant Superintendent had the ability to potentially control all phases of a financial transaction. More specifically, the Assistant Superintendent could enter and approve journal entries, new vendors and purchases.

The Assistant Superintendent told us that he did not realize this access was inappropriate. The Assistant Superintendent stated that the former Assistant Superintendent set up the accounts, and the Assistant Superintendent continued to use them in the same manner in which he was trained when he started at the District.

1 Refer to Appendix B for further information on our sample selection.

We reviewed all activity on both user accounts and identified one transaction in which the Assistant Superintendent entered, approved and issued a purchase order without additional review or approval within the software. We determined this purchase was for an appropriate District purpose. However, when the District has a financial software administrator who is involved in financial operations, it increases the risk that inappropriate transactions could occur and remain undetected.

Unneeded Financial Software User Accounts – Upon our request, the Assistant Superintendent reviewed the 18 financial software user accounts that had not been used in at least 12 months. As a result, the Assistant Superintendent disabled one account because it was for a former business office intern.

The Assistant Superintendent told us that the software is configured to automatically disable accounts when an individual is no longer active on the payroll. However, the intern's account was not automatically disabled because the intern had never been on the District's payroll (the internship was unpaid). Also, the Assistant Superintendent did not have a process for manually reviewing financial software user accounts.

Of the remaining 17 inactive user accounts, 15 generally had limited access to enter budget information and purchase requisitions. The Assistant Superintendent determined that these user accounts were needed, but told us that budget information and purchase requisitions generally were entered into the software by other staff members.

We question the need for these accounts because 12 of the accounts had not been used to access the software in more than four years. The remaining two inactive user accounts were for BOCES staff who could perform District Treasurer duties as needed or when the Deputy Treasurer (who generally performed duties in the financial software) was unavailable. Unneeded user accounts are additional entry points into the financial software and possibly could be used to inappropriately access and view PPSI.

How Does Defining the District's Expectations for Services From Its IT Service Provider Help District Officials Ensure Network and Financial Software Access Controls Are Adequate?

School district officials should ensure they have qualified IT personnel to help adequately control network and financial software access. This can be accomplished by using school district employees, an IT service provider or both.

To protect the school district's network and financial software and avoid potential misunderstandings, officials should have written expectations with the school district's IT service provider that establish the school district's needs, clearly

identify the IT service provider's roles and responsibilities and set the school district's service expectations.

Written expectations help ensure there is mutual understanding between the school district and its service provider for the nature and required level of services to be provided. Officials should monitor the work performed by the IT service provider to ensure the school district receives required, expected services.

District officials did not set defined written expectations with either BOCES. …

District Officials Did Not Adequately Define the Expected Services of Their IT Service Provider

District officials engaged WFL BOCES to provide network support and various services, including support for network access controls. The District also receives financial software support from Monroe 1 BOCES. These services are provided as part of cooperative services agreements, and the District pays WFL BOCES for the services provided by Monroe 1 BOCES through a cross-contract.

District officials did not set defined written expectations with either BOCES to identify the roles, responsibilities and specific services that each was paid to provide. For perspective, the District paid WFL BOCES $539,644 for all IT support and services during the 2020-21 school year.[2] While officials chose BOCES' services by selecting certain items from a list of available BOCES IT services, the lists did not provide detailed explanations of the services. Because the cooperative services agreements do not clearly identify the roles and responsibilities or the nature and required level of services that the vendors will provide, gaps in IT security practices may occur.

Furthermore, officials did not have procedures to monitor and review the work performed by BOCES staff. Therefore, officials could not ensure the District's network and financial software data was adequately safeguarded.

As a result, the District and BOCES did not have stated responsibilities and procedures for network and financial software access controls. This can contribute to confusion over who has responsibility for the various aspects of the District's network and financial software access control management, which could put the District's resources and data at greater risk for unauthorized access, misuse or loss.

2 The District's financial software did not break down costs in detail to obtain the specific cost for only those services directly related to network and financial software access controls.

What Do We Recommend?

The Board should:

1. Set written expectations with BOCES to help ensure that all parties have an understanding of their roles and responsibilities for network and financial software support and services.

2. Ensure officials enforce compliance with the data, network and security access policy.

District officials should:

3. Develop adequate written procedures for managing user account access controls, passwords and remote access and reviewing the network's audit trails.

4. Establish a financial software administrator who is not involved in the financial operations and remove administrative permissions from the Assistant Superintendent so that he does not have the ability to control all phases of a transaction.

5. Disable or remove unnecessary or inappropriate financial software access in a timely manner.

6. Periodically review the financial software user accounts and permissions for necessity and appropriateness.

The IT Director should:

7. Periodically review the network's audit trail for indications of unauthorized or inappropriate network access activity.

8. Disable network user accounts as soon as there is no longer a need for them.

9. Regularly review and update network user accounts for necessity and appropriateness.

Appendix A: Response From District Officials

BLOOMFIELD CENTRAL SCHOOL DISTRICT

Andrew M. Doell, SUPERINTENDENT OF SCHOOLS

45 MAPLE AVENUE, SUITE A, BLOOMFIELD, NY 14469 p: 585-657-6121 EXT. 4004 f: (585) 657-6060 WWW.BLOOMFIELDCSD.ORG

August 19, 2022

Office of the State Comptroller
Edward V. Grant Jr., Chief Examiner
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608

Dear Mr. Grant:

The East Bloomfield Central School District is in receipt of the New York State Office of the Comptroller audit report 2022M-68, which focuses on Network and Financial Software Access Controls. We are pleased to confirm that there is no evidence of malfeasance or fraud. The District views the feedback received from all audits as a way to improve practices. We would like to thank your staff for their professionalism and thorough review.

The District prides itself in being transparent and fiscally responsible. We view our practices for network and financial software access control as a necessary component of this. We are committed to continuous improvement in these areas. The District is in agreement with your findings and is satisfied with the recommendations made.

The District Leadership Team and Board of Education continuously update practices, policies, and procedures including those related to network and financial software access controls. The findings and recommendations will be helpful as we continue work in these areas. The District will develop a corrective action plan in response to your findings and provide that document to your office at a later date.

Thank you again for your feedback.

Sincerely,

Andrew Doell

Superintendent of Schools, East Bloomfield Central School District

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures and interviewed District and BOCES officials to gain an understanding of IT operations and controls, specifically those related to network and financial software access controls.
- We examined network user accounts and permissions using a computerized audit script run on November 23, 2021. We reviewed network user accounts and compared them to current employee lists and student classes to identify inactive and possibly unneeded network user accounts and permissions.
- We examined financial software user accounts and permissions using reports generated from the financial software. We reviewed a list of financial software user accounts and compared the accounts to current employee lists to identify inactive and possibly unneeded financial software user accounts and permissions.
- We inquired with District officials about potentially unneeded user accounts and permissions.
- We reviewed user permissions for eight of the 14 modules (57 percent) in the financial software. We used our professional judgment to select these eight modules based on the higher expected risks – such as permissions that allow users to change financial data or attendance records – that the District would experience if the modules were inappropriately accessed.
- We reviewed financial software user activity reports for activity from July 1, 2020 through January 7, 2022 for two user accounts assigned to the Assistant Superintendent to identify any inappropriate activity.
- We assessed the adequacy of the District's documentation for requested BOCES IT services and determined the cost of those services paid during the 2020-21 school year.

Our audit also examined the adequacy of certain network and financial software access controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller