REPORT OF EXAMINATION | 2018M-164

Bedford Central School District

Information Technology

OCTOBER 2018

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

Contents

Report Highlights

Bedford Central School District

Audit Objective

Determine whether controls over information technology (IT) were properly designed and operating effectively.

Key Findings

- Access to the District's financial application was not properly segregated.
- Online banking users had excessive permissions.
- Employees accessed websites such as shopping, personal email and social networking that did not always comply with the District's Internet use policy.

In addition, sensitive IT control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Ensure that user access to the financial application is properly segregated.
- Limit online banking access to ensure District users cannot control all phases of a transaction.
- Review and adjust the web filtering software to enforce compliance with the District's Internet use policy.

District officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The Bedford Central School District (District) serves the Towns of Bedford, Mount Kisco, New Castle, North Castle and Pound Ridge, in Westchester County.

The District is governed by the Board of Education (Board) which is composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible, along with other administrative staff, for the day-to-day management of the District under the Board's direction. The District's Director of IT is responsible for the oversight and accountability of the District's IT activities and resources.

Quick Facts	
Employees	729
IT Employees	18
Enrollment	4,048
2017-18 Appropriations	$129.1 million

Audit Period

July 1, 2016 – March 5, 2018

We extended our scope forward to May 22, 2018 to complete computer testing.

Information Technology

The District uses IT to initiate, process, record and report financial transactions. It also relies on its IT systems for Internet access, email and maintaining financial, personnel and student records. Therefore, the IT systems and data are valuable District resources. If IT systems are compromised, the results could range from inconvenient to catastrophic and require extensive effort and resources to evaluate and repair.

What Are Effective Financial Application Controls?

Proper segregation of duties is important in any business function but is especially critical for electronic transactions. Without proper segregation of duties, there is an increased risk that one person could commit a wrongdoing and conceal it. Authorizing, transmitting, recording and approving transactions should be segregated and access should be assigned based on the need of the job function. Additionally, audit logs should be reviewed to ensure individuals are making only authorized changes in the application. Any unusual or unauthorized activity could indicate a breakdown in controls or possible malfeasance.

District Users Had Excessive Access to the Financial Application

We found that there is an inadequate user segregation of duties. The Treasurer, along with eight BOCES[1] employees who provide support services, have administrative rights to the financial application.[2] These users have the ability to view, add, delete and modify records in the financial application. For example, the Assistant Superintendent has greater access than necessary because he can enter and approve requisitions which allows him to control all phases of this type of transaction.

Also, 16 users can enter and print checks. Eight of the users are BOCES employees and the remaining users are four secretaries, a part time employee, two account clerks and the bookkeeper. According to the Treasurer, BOCES staff require access to provide support to the District. However, this places the District's funds at risk of theft because these eight users with administrative privileges have access to the District's check stock and could print a District check to cash themselves and conceal it in the system using their administrative access rights.

In addition, District officials do not review the audit log that can be generated from the financial application to ensure individuals are making only authorized

1 Boards of Cooperative Educational Services

2 Because BOCES provides computing services to the District, it is appropriate for certain BOCES to have certain access permissions to the District's IT system and data. However, the appropriateness the access that has been granted to each individual BOCES employees should be evaluated on an individual basis.

changes and to compensate for the inadequate access controls. As a result, there is an increased risk that intentional or unintentional changes could occur without detection.

What Are Effective Online Banking Controls?

New York State General Municipal Law (GML)[3] allows school districts to disburse or transfer funds in their custody by means of electronic wire transfers, provided that the governing board has entered into a written agreement. GML requires that this agreement prescribe the manner in which electronic or wire fund transfers will be accomplished and identify the names and numbers of bank accounts from which such transfers may be made and the individuals authorized to request transfers. In addition, GML requires the district to implement a security procedure that includes verifying that a payment order is for the initiating district and detecting payment order errors in transmission or content. An individual should not be able to execute a wire transfer without obtaining authorization from the custodial officer or a deputy. Municipalities should also check with their banks about enabling alerts and other security measures that may be available such as blocking wire transfers to foreign countries, email notifications and requiring the verification of transactions over certain amounts, possibly through callbacks.

In addition, the board must adopt a policy that outlines the online banking activities district officials will engage in, specifies which employees are authorized to process transactions and establishes a detailed approval process to verify the accuracy and legitimacy of transactions. To the extent possible, authorized users should access bank accounts from one computer dedicated for online banking from a wired network to minimize exposure to malicious software. Other computers may not have the same security protections as a dedicated computer. Officials must segregate duties to ensure that employees are granted access needed to perform their duties but cannot perform all phases of a transaction. The authorization and transmitting functions should be segregated and, if possible, the recording function should be segregated from those functions.

Officials Lacked Adequate Banking Agreements

District officials maintain 13 bank accounts for online transactions, which include electronic deposits, inter-account transfers and automated clearing house (ACH) payments.[4] While the District's banking agreement provided information on the capabilities of performing electronic transfers and security procedures, it did not identify bank account numbers or names of authorized users.

3 Section 5-A

4 ACH is an electronic network used to process large volumes of electronic payments between banks.

In addition, officials did not establish security controls or alerts such as secondary authorizations for online transfers, blocking transfers to foreign countries or email notifications to advise the Treasurer and Assistant Superintendent when transactions occur. Without adequate online banking agreements or security controls, District officials cannot be assured that funds are adequately safeguarded during online banking transactions.

Officials Did Not Adequately Safeguard Online Banking Transactions

The Board did not adopt an online banking policy to establish which employees are authorized to process transactions or establish a detailed approval process to verify the accuracy and legitimacy of transactions before they are processed. In addition, a dedicated separate computer was not used for online banking activities and users had the ability to access online banking from non-district devices. For example, the Treasurer uses non-District devices during vacations to conduct online banking transactions.

Also, four of the six online banking users had excessive permissions because they had the ability to control all phases of online banking transactions. For example, the Treasurer had the ability to initiate, approve and release transactions for 13 District bank accounts without any secondary review or approval. Therefore, we reviewed 25 wire transfers[5] totaling $38.2 million (24 percent) and found that all 25 wire transfers were for appropriate purposes. Additionally, the Treasurer told us that before a wire transfer could be made, the account and beneficiary must be added to the list of approved accounts established by District officials. However, we found one wire transfer totaling $36,000 that, although it was for an appropriate purpose, was transferred to an account that was not on the approved list. District officials were not aware of the excessive permissions that users had in the online banking application. Because the District's claims auditor only reviews wire transfers on a bi-weekly basis, inappropriate transfers could go undetected for an extended period of time without detection.

All online banking users that use either District computers or personal devices are required to use a token that generates a passcode each time the users log in for online banking. However, the District does not have a formal policy to safeguard cash during online banking transactions, prevent online banking from multiple devices or limit banking permissions so that users do not have the ability to control all phases of a transaction. As a result, District officials cannot ensure that employees are aware of their responsibilities and there is an increased risk of unauthorized access, exposure to malicious software, inappropriate activity

5 Two hundred and seventeen wire transfers totaling $157,940,956 were made from July 1, 2016 through February 23, 2018.

and misappropriation of District cash. In addition, there is an increased risk when users access online banking through their personal devices because those devices may not be as secure as the District's computers.

What Are Effective Information Technology Controls?

Internet browsing increases the likelihood of exposure to malicious software that may compromise data confidentiality. Therefore, district officials should use web filtering software to limit vulnerabilities through Internet browsing and ensure the network is used for appropriate purposes. Also, District officials have adopted a technology use policy that limits access to the District's computer network and other technology to education purposes and research consistent with its mission and goals. The policy should prohibit the use of the Internet for non-District approved commercial activity and wastefully using finite District resources.

Disaster recovery is the process to resume business after a disruptive event. District officials should develop a comprehensive disaster recovery plan that addresses the range of threats to their IT system; distribute the plan to all responsible parties; and ensure that it is periodically tested and updated. The plan should focus on sustaining critical business functions during and after a disruption. Given the current and growing threat of ransomware, a strong disaster recovery process is a critical protection to have in place.

The Web Filtering Software Did Not Enforce the Technology Use Policy

We selected and reviewed the web histories for a judgmental sample of 15 of 265 District computers.[6] District staff accessed websites unrelated to District activities, such as shopping, personal email, social networking, travel, ticket purchasing, online bill pay and real estate. This occurred because the District's web filtering software did not block access to these sites to enforce compliance with the District's Internet use policy. In addition, the web filter settings allow potential access to sites in categories including adult products, services and situations, and humor. Inappropriate or questionable use of District computers could potentially expose the District to virus attacks that compromise systems and data, including key financial and confidential information.

6 We selected computers based on employee type and users with access to online banking, financial records and applications containing personal, private and sensitive information (PPSI). Our sample consisted of three Business Office employees, five special education employees, two guidance counselors, four teachers and a psychologist.

The Disaster Recovery Plan Is Not Adequate

While District officials established a disaster recovery plan, it did not address critical business processes for District-wide operations such as disruptions to its IT environment; it only addressed business continuity for the District's financial application. In addition, the plan has not been updated since June 2011 and contains contacts who are no longer employed by the District. The plan includes the former Superintendent and Assistant Superintendent as the primary and secondary contacts for disaster recovery of the District's financial application. District officials also do not periodically test the plan to ensure it is effective. Without a comprehensive and up-to-date disaster recovery plan, District officials do not have adequate guidance on how to react in an emergency and maintain essential business operations.

What Do We Recommend?

The Board should:

1. Adopt a comprehensive online banking policy.

District officials should:

2. Periodically review financial application access rights to ensure that user access to the financial application is properly segregated so that authorizing, transmitting, recording and approving transactions are segregated and that access is based on job function. Particular areas to address include the access granted to eight non-District employees, which includes the ability to enter and print checks.

3. Periodically review the financial application audit log to quickly identify any unusual activity.

4. Ensure that the District has a written agreement with the bank that identifies bank account numbers and names of authorized users and that those who perform online banking transactions are familiar with its content.

5. Enable alerts and other security measures available from the District's bank, including secondary authorizations for online transfers, blocking transfers to foreign countries and email notifications that advise the Treasurer and Assistant Superintendent when online transactions occur.

6. Dedicate a separate computer for online banking activities and limit all online banking to that machine.

7. Periodically review online banking duties and limit access rights to ensure users do not have the ability to control all phases of online banking

transactions. In addition, users should be prevented from making transfers to accounts that are not on the list of approved accounts established by District officials.

8. Review and adjust the web filtering software to enforce compliance with the technology use policy.

9. Develop a comprehensive disaster recovery plan, and update and test the plan periodically.

Appendix A: Response From District Officials

Bedford Central School District
Inspiring and Challenging Our Students

Dr. Christopher M. Manno
Superintendent of Schools
cmanno4173@bcsdny.org
Phone: (914) 241-6000

October 5, 2018

Tenneh Blamah
Chief Examiner of Local Government and School Accountability
Office of the State Comptroller

Dear Ms. Tenneh Blamah:

Thank you for providing the comprehensive audit report focused on our Information Technology program and fiscal controls. The findings and recommendations will assist the District in more effectively executing our fiduciary responsibilities and protecting our technology network and infrastructure.

The District offers the following responses to the findings and recommendations included in the Information Technology Report of Examination, 2018M-164.

I. Access to the District's financial application was not properly segregated. District users had excessive access to the District financial application.
   A. The District will conduct an initial comprehensive access review of all BCSD and BOCES employees and adjust permissions to ensure that user access to the financial application is properly segregated so that authorizing, transmitting, recording and approving transactions are segregated and that access is based on job function. Particular areas to address include the access granted to eight non-District employees, which includes the ability to enter and print checks.
   B. The District will periodically review financial application access rights and the financial application audit log to quickly identify any unusual activity.

II. Officials lacked adequate banking agreements.
   A. District officials will revise the written agreement with the bank to identify bank account numbers and names.
   B. District officials will ensure authorized users and those who perform online banking transactions are familiar with the content of the agreement.
   C. Investigate the measures or tools available to enable alerts and other security measures from the District's bank, including secondary authorizations for online transfers, blocking transfers to foreign countries, and email notifications that advise the Treasurer and Assistant Superintendent when online transactions occur.

III. Online banking users had excessive permissions. Officials did not adequately safeguard online banking transactions.

Bedford Central School District
Fox Lane Campus
P.O. Box 180
Mt. Kisco, NY 10549

Dr. Christopher M. Manno
Superintendent of Schools
cmanno4173@bcsdny.org

A. The Board should adopt a comprehensive online banking policy to establish which employees are permitted to process transactions, limit the devices from which transactions may occur, and segregate duties to ensure employees are granted only the access needed to perform their duties.
B. District Officials should dedicate a separate computer for online banking activities and limit all online banking to that machine, except in limited circumstances requiring additional controls.
C. District officials periodically review online banking duties and limit access rights to ensure users do not have the ability to control all phases of online banking transactions. In addition, users should be prevented from making transfers to accounts that are not on the list of approved accounts established by District officials.

IV. Employees accessed websites such as shopping, personal email and social networking that did not always comply with the District's Technology Use Policy. The web filtering software did not enforce the Technology Use Policy.
A. Review and revise the Staff Acceptable Use Policy to conform with current best practices and to balance the need for staff technology use for instructional and effective communication/community engagement purposes with the efficient and effective operations of the District.
B. Review and adjust the web filtering software to enforce compliance with the Technology Use Policy.

V. The Disaster Recovery Plan is not adequate.
A. Develop a comprehensive disaster recovery plan, and update and test the plan periodically.
B. Ensure the Disaster Recovery Plan prevents disruption in critical business and IT processes, and update contact information.

Again, we appreciate your thoughtful and detailed analysis and your assistance in promoting effective and efficient management and operations of the Bedford Central School District. We will create the required Corrective Action Plan and submit it within 90 days of the release of the audit.

Sincerely,

Dr. Christopher Manno,
Superintendent of Schools

Mrs. Colette Dow,
President, BCSD BoE

c: Board of Education
Ms. Nancy Sasso, Treasurer
Mr. David Gee, Director of Technology

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 policy and procedure manuals to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed officials and personnel to gain an understanding of internal controls over IT and online banking.
- We reviewed the user access rights for the District's financial application and evaluated permissions to determine whether user access is properly segregated and based on the need of the job function.
- We inquired about a written agreement with the District's bank and an online banking policy. We also reviewed documentation regarding capabilities for electronic transfers.
- We reviewed user access rights for the online banking application and evaluated permissions to determine whether there was a proper segregation access rights and if the granted access rights were necessary for employees to perform their assigned duties.
- We judgmentally selected a sample of 25 of the 217 wire transfers made during our audit period to determine whether they were for appropriate purposes and to approved beneficiaries. Our sample selection was based on vendor name, payment frequencies and payment amount.
- We judgmentally selected a sample of 15 computers for the 265 users who had access to PPSI.[7] We reviewed web history reports for accessed websites that violated the District's Internet use policy or could put the network at risk. We selected those assigned to the Treasurer, bookkeeper and payroll clerk because their duties and privileges involved using and transmitting important electronic financial data. We also selected 12 computers used by school level employees (special education, guidance counselors, teachers and a psychologist).
- We reviewed the District's disaster recovery plan and assessed its adequacy.

Our audit also examined the adequacy of certain information technology 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.

7 These users had access to key financial applications and related PPSI including online banking, payroll, human resources, vendors and students.

We conducted this performance audit in accordance with GAGAS (generally accepted government auditing standards). 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.

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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.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/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

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

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/localgov/index.htm

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

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

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