DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2018M-74

Dundee Central School District

Information Technology

AUGUST 2018

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

Contents

Report Highlights

Dundee Central School District

Audit Objective

Determine whether the Board and District Officials ensured District information technology (IT) assets and computerized data were safeguarded.

Key Findings

- The Board and District officials have not adopted adequate IT security policies and procedures.
- District officials did not provide IT security awareness training for District employees.

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

Key Recommendations

- The Board and District officials should adopt comprehensive IT security policies, procedures and plans to safeguard computerized assets and data.
- Provide periodic IT security awareness training to personnel who use IT resources.

District officials generally agreed with our recommendations and indicated they are in the process of taking corrective action.

Background

The Dundee Central School District (District) serves the Towns of Starkey, Barrington and Milo in Yates County and the Towns of Reading and Tyrone in Schuyler County. The District is governed by a seven-member Board of Education (Board) responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the chief executive officer responsible for the District's administration. The Business Administrator is the chief fiscal officer. The IT Director is responsible, along with two technicians, for the overall management of the District's IT infrastructure; they serve as the network administrators.

Quick Facts	
Number of Students	Approximately 700
Number of Staff	Approximately 200
Number of Desktops, Laptops and Tablets	Approximately 1,030

Audit Period

July 1, 2016 – January 29, 2018

Information Technology

The District relies on its IT assets for Internet access, email and for maintaining confidential and sensitive financial, personnel and student records. The District recently made a significant investment in IT upgrades through the Smart Schools Bond Act, which resulted in the assignment of desktops, laptops, and tablets to almost all students, educational staff and District employees. If the IT assets are compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of assets and data, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. Wayne Finger Lake BOCES handles the District's internet filtering and firewall/intrusion detection.

What Policies and Procedures Should the Board Adopt to Safeguard IT Assets and Data?

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential for the Board to establish IT security policies for all IT assets and information.

The District should have acceptable computer use policies that define the procedures for computer, Internet and email use and include IT security awareness training requirements for staff. Additionally, the District should adopt policies and procedures for data classification, the use of and access to personal, private and sensitive information (PPSI), password security, wireless security, user accounts and access rights, remote access, online banking, sanitation and disposal of IT equipment, and backups and disaster recovery. The Board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies.

The Board Did Not Adopt and District Officials Did Not Enforce Adequate IT Security Policies and Procedures

While the District has acceptable use policies, they are not monitored or enforced. In addition, the policies do not address connecting personal mobile computing and storage devices to the District's network. Connecting personal devices to the District's network can create security vulnerabilities and allow inappropriate access to District IT assets and data. Further, the District's staff acceptable use policy does not require cybersecurity training.[1]

Acceptable use policies are not monitored or enforced.

[1] Refer to "Why Should District Officials Provide IT Security Awareness Training?" section of report.

We reviewed 25 users' web histories on 20 District computers[2] and found questionable Internet use for seven users, such as online gaming, shopping and banking, use of personal email and social networking sites, and visiting travel, news and entertainment and job searching websites.

The Board has not adopted other IT security policies addressing password management, protection of PPSI,[3] wireless technology, remote access, sanitation and disposal of electronic media, user accounts, access rights, online banking and data backups. While IT policies will not guarantee the safety of the District's IT assets and data, a lack of appropriate policies significantly increases the risk that data, hardware and software may be lost or damaged by inappropriate use or access. Without formal policies that explicitly convey the appropriate use of the District's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

Why Should District Officials Provide IT Security Awareness Training?

Computer users must be aware of security risks and trained in practices that reduce internal and external threats to IT systems and data. While IT policies tell computer users what to do, IT security awareness training helps them understand their roles and responsibilities and provides them with the skills to perform them. Such training should center on:

- Emerging trends in information theft and other social engineering reminders;
- Limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed;
- Malicious software, virus protection and the dangers of downloading files and programs from the Internet;
- Password controls; and
- The restriction of physical access to IT systems and resources and how to protect them from intentional or unintentional harm, loss or compromise.

District Employees Are Not Provided IT Security Awareness Training

District officials did not provide users with IT security awareness training to help ensure they understand IT security measures. As a result, the District's IT assets and data are more vulnerable to loss and misuse. For example, during our review

[2] Refer to Appendix B for further information on our sample selection.

[3] Such as practices to safeguard when collecting, storing or transmitting PPSI information

of District IT assets, we noted the District's IT systems for HVAC and public address speakers were accessible through the unlocked maintenance office and the usernames and passwords for the HVAC systems were written on sticky notes on the side of the desktop computer. We also observed staff usernames and passwords written on sticky notes stuck to their computing devices. In addition, we observed IT hardware, such as keyboards and monitors sitting on the floor in an elementary teachers' lounge, and a desktop computer sitting on the floor of the counseling office. Lastly, we noted that users' recycle bins were not set to automatically empty, which resulted in four users' recycle bins containing large amounts of files, some as old as 2013, and two of these users' recycle bins contained possible PPSI.

Why Should the District Have a Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event[4] that compromises the availability or integrity of an IT system and data. Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure they will function as expected.

The District Does Not Have a Disaster Recovery Plan

The Board did not develop a formal disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, District officials have no guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data. Without a disaster recovery plan, the District could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process grades and state aid claims.

Why Should the District Maintain Up-to-Date Hardware Inventory Records?

District officials should maintain detailed, up-to-date inventory records for all computer hardware to safeguard IT assets. Information maintained for each piece of computer equipment should include a description of the item, name of

[4] Such as a fire, computer virus or inadvertent employee action

the employee or student to whom the equipment is assigned, physical location of the equipment and relevant purchase or lease information. Officials should verify the accuracy of inventory records through periodic physical inventory counts. Maintaining a complete and up-to-date hardware inventory aids the Board's development and formalization of an IT replacement plan.

Hardware Inventory Records Were Outdated

The IT Director maintained a hardware inventory for the District, however, it was not up-to-date at the time of our audit. Upon our request, the IT Director updated the hardware inventory for our use.

Organizations cannot properly protect IT resources if personnel are unaware of existing resources and where those resources reside. Because District officials did not maintain up-to-date hardware inventory records, the District has an increased risk that its IT assets may be lost, stolen or misused. Further, the Board's ability to develop a formalized IT replacement plan was hindered.

What Are Strong Access Controls?

District officials are responsible for restricting users' access to just those applications, resources and data that are necessary for their day-to-day learning, duties and responsibilities to provide reasonable assurance that computer resources are protected from unauthorized use or modifications. User accounts enable the system to recognize specific users, grant the appropriately authorized access rights and provide user accountability by affiliating user accounts with specific users, not sharing user accounts among multiple users and disabling generic user accounts. Users with administrative rights and remote access must also be limited and all user access should be monitored. Finally, all users should set their own passwords within prescribed requirements. Holding passwords to certain complexity, length and age requirements makes passwords more difficult to crack or be easily guessed.

District Officials Did Not Implement Strong Access Controls

The District has not implemented comprehensive procedures for managing, limiting, securing and monitoring user access. As a result, we noted inactive user accounts, excessive administrator user accounts and inadequate password requirements. For example, a total of 622 of the 1,257 users (49 percent) have not been used in the last six months and 40 of the 1,257 users (3 percent) do not match current employees. Consequently, the District's IT assets and data are at increased risk for loss or misuse.

What Do We Recommend?

The Board should:

1. Update the acceptable use policies to limit connecting personal mobile computing and storage devices and include provisions for IT security awareness training.

2. Adopt comprehensive IT security policies addressing password management, protection of personal, private, sensitive information, wireless technology, remote access, sanitation and disposal of electronic media, user accounts, access rights, online banking and data backups.

3. Periodically review and update all IT policies and procedures to reflect changes in technology and the District's computing environment and stipulate who is responsible for monitoring all IT policies.

4. Develop and adopt a comprehensive disaster recovery plan, including backup procedures and offsite storage.

5. Develop a formalized IT replacement plan.

District officials should:

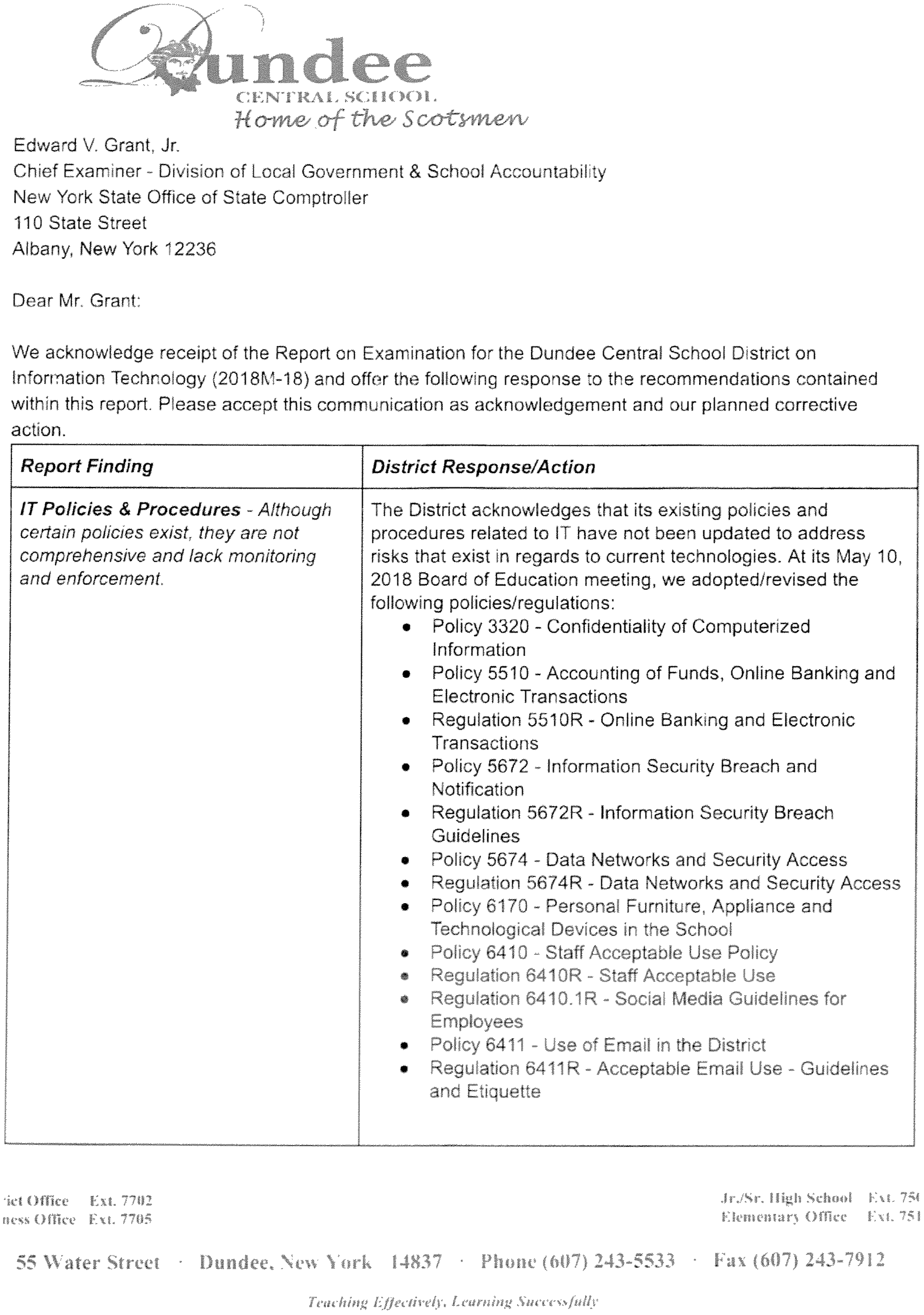
6. Develop procedures for monitoring internet usage and enforcing the acceptable use policies.

7. Provide periodic IT security awareness training to personnel who use IT resources, including the importance of physical security and protection of PPSI.

8. Maintain an up-to-date hardware inventory.

9. Develop comprehensive procedures for managing, limiting, securing and monitoring user access.

Appendix A: Response From District Officials



Dundee
CENTRAL SCHOOL
Home of the Scotsmen

Edward V. Grant, Jr.
Chief Examiner - Division of Local Government & School Accountability
New York State Office of State Comptroller
110 State Street
Albany, New York 12236

Dear Mr. Grant:

We acknowledge receipt of the Report on Examination for the Dundee Central School District on Information Technology (2018M-18) and offer the following response to the recommendations contained within this report. Please accept this communication as acknowledgement and our planned corrective action.

See
Note 1
Page 10

Report Finding	***District Response/Action***
IT Policies & Procedures *- Although certain policies exist, they are not comprehensive and lack monitoring and enforcement.*	The District acknowledges that its existing policies and procedures related to IT have not been updated to address risks that exist in regards to current technologies. At its May 10, 2018 Board of Education meeting, we adopted/revised the following policies/regulations: • Policy 3320 - Confidentiality of Computerized Information • Policy 5510 - Accounting of Funds, Online Banking and Electronic Transactions • Regulation 5510R - Online Banking and Electronic Transactions • Policy 5672 - Information Security Breach and Notification • Regulation 5672R - Information Security Breach Guidelines • Policy 5674 - Data Networks and Security Access • Regulation 5674R - Data Networks and Security Access • Policy 6170 - Personal Furniture, Appliance and Technological Devices in the School • Policy 6410 - Staff Acceptable Use Policy • Regulation 6410R - Staff Acceptable Use • Regulation 6410.1R - Social Media Guidelines for Employees • Policy 6411 - Use of Email in the District • Regulation 6411R - Acceptable Email Use - Guidelines and Etiquette

ict Office Ext. 7702
ness Office Ext. 7705

Jr./Sr. High School Ext. 75(
Elementary Office Ext. 751

55 Water Street · Dundee, New York 14837 · Phone (607) 243-5533 · Fax (607) 243-7912

Teaching Effectively, Learning Successfully

IT Policies & Procedures, con't.	Monitoring and enforcement of current and now adopted policies and procedures will be conducted or enforced beginning September 2018 in the following ways based on area of concern: ● Password (Complexity) - Adoption of Policy 5674 and Regulation 5674R state the need for passwords to meet complexity requirements and we will be enforcing these for all user accounts through our Active Directory infrastructure with new Group Policy objects. These will be developed and deployed before opening conference days that start August 27, 2018. ● Acceptable Use Policy(s) Enforcement - Will be monitored by a monthly selection of random staff members devices and student devices starting in September 2018 where we will review internet history and potential careless use of PPSI data on said devices. ● Policies and regulations will be used in determining if users have complied with our district AUP(s). The results of monthly *checks* conducted by the technology staff will be recorded and any findings of non-compliance will be brought to the attention of appropriate administration in the school district.
IT Security Awareness Training *-The District does not provide adequate IT security awareness training for IT users*	The school district will include IT security training as part of its opening conference days held prior to the start of each school year. For 2018-2019 this date is August 27, 2018. This training will be mandatory for all school district staff. Additionally, new staff who become employed during the school year will also receive the IT security training as part of their employment orientation. This training will be conducted by the school district's IT staff. Training will also include an annual review of the district AUP(s) and require staff member's signature annually prior to issuance of any device. In addition beginning in September 2018 district technology staff will be producing a monthly video series featuring How-To's and Best Practices that will available to all employees and Board members.
Disaster Recovery Plan *-The District does not have a current Disaster Recovery Plan to address potential disasters.*	The school district is working on developing a Critical Function & Continuity of Operations Plan that will provide a response system to use in the event of a critical technological failure in the district; its goal is to recover essential electronic data in the shortest amount of time. This comprehensive plan is being drafted by the school district administration and we anticipate it will be completed by March 31, 2019. This will be coordinated with the Data Classification policy development and adoption and updating of hardware inventory records.

Hardware Inventory Records *-A current inventory of hardware was not maintained prior to the examination*	The school district has updated its hardware and software inventory records and provide these to the audit team during the examination and will continue to maintain this on an ongoing basis to reflect acquisitions and dispositions..The System Analyst, Computer Technician and Computer Aide will annually provide this inventory to the school business office for insurance purposes in the Fall/Spring of each year. A physical inventory will be verified during October 2018 by the district technology staff to insure accuracy of these records.
User Access Controls *-The District does not have adequate procedures for managing user access*	The school district has adopted policies and regulations that will guide users in the use of technology. The school district administration is developing a Data Classification policy and anticipates it will be developed and Board approved by September 30, 2019. The Data Classification policy will be used in determining district user access/permissions to district data. The policy will classify *data* as either Public, Sensitive or Restricted and break down the type of data accessed by district employee position. In April 2018 the technology staff took steps to update its current user directories by verifying active users, disabling inactive users, including those with no activity within the last six months. In conjunction with developing the Data Classification policy the district will be developing procedures for staff to follow in notifying district technology staff when changes to users or user permissions are necessary.
Technology Replacement Plan *-The District does not have an active technology replacement plan*	The school district prepared a spreadsheet in May 2018 that includes quantities and device types projected for the next five years, resulting in full inventory turnover over the course of the plan for both students and staff. This plan will be presented to the Board of Education during January/February 2019 for approval. This plan will be expanded to include network infrastructure projections by October 1, 2019.

We believe these actions will contribute to our goal to protect the confidentiality of data, to preserve the integrity of data and to promote the availability of data for authorized use, while protecting our assets and clearly setting forth acceptable and unacceptable behaviors.

This plan has been reviewed and approved by the Board of Education at its regular meeting on July 9, 2018.

Respectfully submitted,

Dundee Central School District

Appendix B: OSC Comments on the District's Response

Note 1

The report number referenced in the District's response has been changed to 2018M-74.

Appendix C: 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 adopted IT policies and procedures and interviewed District officials to gain an understanding of the District's IT operations and determine the adequacy of the District's IT policies and procedures.
- We examined the District's Active Directory settings using specialized audit software. We reviewed the user and administrator accounts and compared them to current employee lists to identify inactive and unnecessary accounts. Further, we reviewed group policy automated settings and compared them to best practices.
- From various permissions reports we identified users and administrative permissions for the financial and special education management software. Then using Active Directory information we placed the various Active Directory users' information in a pivot table. Using this pivot table we pulled out the student management system (SMS) and Active Directory administrators and users. We combined the user and administrator information for Active Directory, SMS, and financial and special education management software into one table. We then assigned a risk score to the various users based on the applications' they had access to, whether they were administrators of the software applications and if the software applications they accessed contained PPSI. We categorized the users into various risk levels (Very High Risk, High Risk, Medium Risk and Low Risk) based on the risk score. We judgmentally selected a sample size for each risk category and randomly selected the users for the computer testing sample.

Figure 1: Test Sample

	Number of Users	Percentage of Total Population	Number of Users Sampled	Percentage of Sample Users
Very High Risk	7	0.5%	7	100%
High Risk	72	5.5%	20	28%
Medium Risk	10	1%	3	30%
Low Risk	1,196	93%	5	0.4%
Total	**1,285**	**100%**	**35**	**3%**

- We used specialized audit software to obtain web histories, installed software and device settings for all 35 computers tested. We reviewed the device settings for these computers. Because of the large number of software installations and web histories, we analyzed the results for 20 of the computers to determine if they served a legitimate business purpose or presented any risk to the District's IT system. In addition we reviewed every fifth computer of the listed 35 sampled computers for specific file extensions to determine if the computer was being used on a more than incidental basis for personal use and whether PPSI was protected.
- We compared identifiers for the sampled computers tested to the District's IT hardware inventory.
- During the performance of our testing we walked throughout the District's facilities and made observations of physical security controls.

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.

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 District Clerk's office.

Appendix D: 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

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, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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