OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Village of Westhampton Beach

Internal Controls Over Information Technology

Report of Examination

Period Covered:

June 1, 2011 — April 30, 2013

2013M-173

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

August 2013

Dear Village Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and Board of Trustees governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit of the Village of Westhampton Beach, entitled Internal Controls Over Information Technology. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

This audit's results and recommendations are resources for local government officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The Village of Westhampton Beach is located in the Town of Southampton, in Suffolk County, and has a population of approximately 1,500 residents. The Village is governed by a Board of Trustees (Board) which comprises four elected Trustees and an elected Mayor. Budgeted appropriations for the 2012-13 fiscal year were approximately $9.4 million, funded primarily through real property taxes.

The Board is responsible for the general management and controls of the Village's financial affairs, which includes establishing comprehensive policies and procedures to safeguard Village computer assets. The Village does not have information technology (IT) staff and contracts with a vendor to assist employees with any computer-related problems.

Objective

The objective of our audit was to review the Village's internal controls over IT. Our audit addressed the following related question:

- Are internal controls over IT appropriately designed and operating effectively to ensure that electronic data is adequately safeguarded?

Scope and Methodology

We evaluated the Village's oversight of IT for the period June 1, 2011, to April 30, 2013. Our audit disclosed areas where additional IT security controls should be instituted. Because of the sensitive nature of some of this information, certain specific vulnerabilities are not discussed in this report, but have been separately communicated to Village officials so they could take corrective action.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report.

Comments of Local Officials and Corrective Action

The results of our audit and recommendations have been discussed with Village officials and their comments, which appear in Appendix A, have been considered in preparing this report. Village officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded

to our office within 90 days, pursuant to Section 35 of the General Municipal Law. 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 this plan available for public review in the Clerk's office.

Information Technology

The Village relies on its IT system for accessing the Internet, communicating by email, storing data, and recording financial information. Therefore, the Village's IT system and the data it holds are valuable resources. If the IT system fails, the results could range from inconvenient to severe. Even small disruptions in IT systems can require extensive effort to evaluate and repair. Village officials are responsible for developing written policies and procedures to effectively safeguard IT resources. Such policies and procedures should address using and monitoring the Village's IT system and developing a formal disaster recovery plan to reduce the risk of data loss and to provide guidance to staff on its recovery in the event of a disaster.

Village officials have not developed formal IT policies for user access, and the Board has not developed a formal disaster recovery plan. We found generic user accounts on the Village's computer system and some users unnecessarily had administrative rights. We also found that the Village Clerk/Treasurer has administrative rights to the Village's financial software. Therefore, she has the ability to add users, modify access rights and data files, and correct errors. Finally, although audit logs are available through the financial software, they are not generated and reviewed by Village officials. As a result of these weaknesses, the Village's IT system and its data are subject to an increased risk of corruption, loss, or misuse.

Network User Accounts

Network access controls limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and disclosure. User identifiers (IDs) and passwords are the simplest and most common forms of user authentication to prevent unauthorized use or modification. User IDs enable the system to recognize specific user accounts, grant the appropriately authorized access rights, and provide user accountability for computer transactions. If user IDs are not affiliated with a specific user, but instead are shared among multiple users, Village officials are unable to determine responsibility for system activities. Users with administrative access can assign user rights and access control permissions as necessary. Administrators can install and uninstall applications and make adjustments to security and system settings at will.

Village officials have not established policies and procedures to ensure proper controls over user access to the Village's network. We reviewed all 50 user access accounts on the network and found the

Village has eight generic user accounts, which are used by multiple users, four of which had administrative rights to the server. The use of generic user accounts and granting unnecessary administrative rights to users makes the system vulnerable and limits Village officials' ability to determine responsibility for system activities. The ability to potentially download and install unauthorized software increases the risk that sensitive or critical data may be lost or compromised.

Financial Application User Access

Effective controls over access rights to a financial software application should allow users access to only those computerized functions that are consistent with their job responsibilities and should prevent users from being involved in multiple aspects of financial transactions. An individual who has financial system administrative rights can add new users, create and change user access rights, configure certain system settings, and override management controls. Accordingly, the financial system administrator should not be involved in the Village's financial operations. Village officials must ensure that user access rights are appropriate to employees' job descriptions and levels of responsibility and that those rights are promptly adjusted or deactivated when employees' responsibilities change.

Village officials did not ensure that access to the Village's financial software application is restricted to only those functions required by individual employees' job duties. We reviewed the permissions granted to financial software users and found that the Clerk/Treasurer has administrative rights to the Village's financial application. With administrative rights, the Clerk/Treasurer is able to control and use all aspects of the financial software applications, including creating a new user, updating the user access rights, and performing other administrative functions including management overrides. With these abilities, she could create fictitious users to misappropriate Village funds.

Audit Logs

An audit log is an automated mechanism for establishing individual accountability, reconstructing events, and monitoring problems. An audit log maintains a record of activity by computer system or application that identifies each person who accesses the system, records the time and date of the access, identifies the activity that occurred, and records the time and date of log-off. Village officials should review audit logs to monitor the activity of persons who access Village accounting records and to identify problems that may have occurred.

Village officials told us that their financial software system has the ability to generate audit logs. However, this system feature is not being used. Because Village officials have not implemented procedures to periodically produce and review these logs, the ability to detect and address unauthorized activities is compromised.

The combination of the user access issues and failure of Village officials to examine audit logs could allow individuals to initiate improper transactions and misappropriate funds without detection. Given that virtually all Village financial records and reports are computer generated, the risk is substantial.

Disaster Recovery Plan

A disaster recovery plan provides a framework for reconstructing vital operations to ensure the resumption of time-sensitive operations and services in the event of an emergency. A strong system of internal controls includes a disaster recovery plan that describes how the Village plans to deal with potential disasters. Such disasters may include any sudden, catastrophic event (e.g., fire, computer virus, power outage, or a deliberate or inadvertent employee action) that compromises the availability or integrity of the IT system and data. The plan should describe the precautions to be taken to minimize the effects of a disaster and enable the Village to either maintain or quickly resume critical functions. The plan should include a significant focus on disaster prevention and should be distributed to all responsible parties, periodically tested, and updated as needed.

The Board has not developed a formal disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, Village personnel have no guidelines or plan to follow to help minimize or prevent the loss of equipment and data or guidance on how to implement data recovery procedures. Further, without a disaster recovery plan, the Village is at risk for the loss of important data and the disruption of time-sensitive operations.

Recommendations

1. The Board should establish a policy to ensure that access to the IT system and financial software application is provided to a specified person based on the needs associated with their job functions. All generic user accounts should be removed, and administrative rights should be restricted to only those individuals who need them.

2. Village officials should ensure that administrative rights to the financial software are not given to someone involved in financial operations.

3. Village officials should routinely generate and review the financial software audit logs to monitor user activity, including the potential threat of unauthorized access by third parties.

4. The Board should establish a formal disaster recovery plan that addresses the range of potential threats to the Village's IT systems and data and provides the guidance necessary to maintain Village operations or restore them as quickly as possible in the event of a

disaster. This plan should be distributed to all responsible parties, periodically tested, and updated as needed.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

The local officials' response to this audit can be found on the following page.

Incorporated Village of Westhampton Beach
165 Mill Road, Westhampton Beach, New York 11978
Phone: (631) 288-1654 * Fax: (631) 288-4332
info@westhamptonbeach.org

August 21, 2013

Ira McCracken, Chief Examiner
Division of Local Government and
School Accountability
NYS Office Building
Room 3A10
Veterans Memorial Highway
Hauppauge, NY 11788-5533

Dear Mr. McCracken:

I am writing to you in response regarding the Village of Westhampton Beach Internal Controls over Information Technology Report of Examination; I agree with the report findings and have started implementing the changes noted in the report.

Sincerely

Conrad W. Teller
Mayor

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard Village assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: financial oversight, cash receipts and disbursements, purchasing, information technology (IT), payroll and personal services, and the internal operations of the individual Village departments.

During the initial assessment, we interviewed appropriate Village officials, performed limited tests of transactions, and reviewed pertinent documents, such as Board minutes and financial records and reports. Further, we reviewed the Village's internal controls and procedures over the computerized financial databases to help ensure that the information produced by such systems was reliable.

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed and evaluated those weaknesses for the risk of potential fraud, theft and/or professional misconduct. We then decided on the reported objective and scope by selecting for audit those areas most at risk. We selected IT for further audit testing.

To accomplish our audit objective and to obtain valid audit evidence, our audit procedures for IT included the following:

- We reviewed the Village's IT policies and procedures.

- We interviewed the Village Clerk/Treasurer and the Village's contracted IT vendor regarding the IT system and financial software. This included inquiries regarding default accounts, user access, audit logs, and disaster recovery procedures.

- We obtained a list of all the users of the financial software and their access rights to determine if their access to the financial software was consistent with their job responsibilities. We also reviewed the list to determine if default accounts had been removed and only active employees had access to the software.

- Through manual examination, we tested Villages computers and servers by running audit software and examining the IT controls over the system.

- We examined the server rooms and server rack for physical security.

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.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Nathaalie N. Carey, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Robert Meller, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

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

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

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

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313