



City of Norwich Information Technology

Report of Examination

Period Covered:

January 1, 2011 — September 5, 2012

2012M-254



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	2
INTRODUCTION	3
Background	3
Objective	3
Scope and Methodology	3
Comments of Local Officials and Corrective Action	4
INFORMATION TECHNOLOGY	5
Server Location	5
Administrative Privileges	5
Disaster Recovery Plan	6
Recommendations	6
APPENDIX A Response From Local Officials	7
APPENDIX B Audit Methodology and Standards	9
APPENDIX C How to Obtain Additional Copies of the Report	10
APPENDIX D Local Regional Office Listing	11

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

February 2013

Dear City 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 City Council 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 City of Norwich, entitled 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 City of Norwich is located in Chenango County. The City has 7,190 residents. The City is governed by a six-member Common Council (Council). The Council is responsible for the general management and control of the City's assets, including computerized data and assets. As such, it is responsible for establishing policies that govern the use and protection of computerized data and assets. The Mayor is responsible for establishing day-to-day procedures and controls to ensure that the Council's policies are enforced and to protect the computerized data and assets, including the servers. The City Director of Finance (Director) oversees the City's information technology (IT). The Mayor and the Director are jointly responsible for ensuring that users of the system adhere to adopted policies and procedures.

The City's 2012 budget for the general fund was approximately \$7.6 million, funded mainly from real property taxes, sales and use taxes, and State aid. The primary services financed by the general fund are police and fire, street maintenance and repair, youth programs, and general government support.

Objective

The objective of our audit was to determine if computerized data and assets were properly safeguarded. Our audit addressed the following related question:

- Did City officials ensure that computerized data and assets were properly safeguarded?

Scope and Methodology

We examined internal controls relating to the City's computerized data and assets for the period January 1, 2011 to September 5, 2012. Our audit disclosed additional areas in need of improvement concerning IT controls. Because of the sensitivity of some of this information, certain vulnerabilities are not discussed in this report, but have been communicated confidentially to City officials so they can 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 City officials and their comments, which appear in Appendix A, have been considered in preparing this report. City officials generally agreed with our audit findings 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 City Common Council to make this plan available for public review in the City Clerk's office.

Information Technology

The City's information technology (IT) system is a valuable and essential part of operations, used for accessing the Internet, communicating by email, processing and storing data, maintaining financial records, and reporting to state and federal agencies. Therefore, it is imperative that the City's computerized data is properly safeguarded. The Mayor and Director should ensure that the City's servers are located in a secure and safe location. Additionally, the system should include a disaster recovery plan to prevent the loss of computerized data and assets and to ensure that operations can resume in the event of a power outage or disaster.

The City's servers are not placed in secure locations. In addition, system users were granted administrative privileges that they did not need to perform their job duties. Further, the Council has not adopted a disaster recovery plan. As a result, there is an increased risk that computerized data could be lost or compromised, or that City operations could be seriously disrupted.

Server Location

The Mayor and Director must provide for the proper location of servers and implement procedures to ensure that only authorized staff members can gain physical access to servers.

The City's servers are located in the City Clerk's office and sit on the floor. We observed that this office is not always secured and locked. When the Clerk was at his desk, the servers were somewhat protected. However, he was often away from his desk. In some cases, the office was completely empty and the door to the office was wide open. City officials explained that, at one time, the Clerk's office was a secured server room that contained only the servers. However, due to space constraints, the server room became the Clerk's office. If access to the servers is not controlled, the risk increases that unauthorized access to the network could be obtained and the servers could be damaged.

Administrative Privileges

Users with administrative privileges have the ability to add and remove software at their discretion, change configuration settings, and add and remove local users. In other words, administrators have complete control over their local workstation. City officials must limit administrative privileges to minimize both the spread of malicious software (malware) and the risk to data.

We identified weaknesses in the City's assignment of administrative privileges. Because City officials failed to correct these issues at the

time of our exit conference, we communicated the findings in the confidential IT letter for security reasons.

Disaster Recovery Plan

The City's IT system is a critical resource that must be adequately protected against loss, damage, or misuse. An effective internal control system for IT requires a formal disaster recovery plan (DRP) to prevent the potential loss of computer resources, and to outline procedures for the recovery of data in the event of a disaster. A DRP, sometimes referred to as a business continuity plan or business process contingency plan, describes how an organization must deal with potential disasters. It describes the precautions that must be taken to minimize the effects of a disaster, enable the organization to restore data, and either maintain or quickly resume its mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs, and may include a significant focus on disaster prevention.

The Council has not developed a DRP. Consequently, in the event of a disaster, City 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 and resume operations as efficiently as possible. The lack of a DRP could lead to loss of important financial data along with a serious interruption to City operations, such as not being able to process checks to pay vendors or employees.

Recommendations

1. The Mayor should move the City's servers so that only authorized staff members can gain access.
2. City officials should limit the assignment of administrative privileges to only those users who require such access to perform their job duties.
3. The Mayor should work with the Council to develop a DRP. The Council should then adopt the DRP and its elements.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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



February 14, 2013

H. Todd Eames, Chief Examiner
Office of the State Comptroller
Binghamton Regional Office
State Office Building, Room 1702
44 Hawley Street
Binghamton, New York 13901-4417

Re: Information Technology
Report of Examination 2012M - 254
for January 1, 2011 – September 5, 2012

Dear Mr. Eames:

We have reviewed the subject audit report prepared by your office regarding the determination of whether computerized data and associated information technology assets of the City of Norwich were properly safeguarded.

We believe the report accurately reflects the pertinent IT security status and discloses the need for improvements and corresponding corrective actions. We therefore wish to advise you that we fully concur with all of the report's recommendations. We have met with our IT support provider, with whom we contract for full hardware support services, as well as software and related security provisions. Measures will be taken to ensure that both physical security and appropriate controls over the access to sensitive data are implemented in fulfillment of the report's recommendations.

In follow up to this response, we will be timely filing a Corrective Action Plan (CAP) with you, following its review and approval by our Common Council. In the meantime, we wish to express our sincere appreciation for the very professional and helpful assistance that all of the staff members from your office have provided us in this process. We have always highly regarded the valuable resource that the Binghamton Regional Office represents to us, and we feel that this particularly important assessment would have been quite costly for us to have acquired through outside means.

Sincerely yours,
City of Norwich

Joseph P. Maiurano
Mayor

William J. Roberts
Director of Finance / City Clerk

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

During this audit, we examined the City's information technology (IT) system. To accomplish our audit objective and obtain relevant audit evidence, our procedures included the following:

- We conducted in-person interviews with various City officials and employees to gain an understanding of the controls over the IT system.
- We inspected and observed City operations regarding the City's IT hardware.
- We ran a workstation auditing tool on selected workstations to collect security configurations, group membership, and user settings.

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
Steven J. Hancox, 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-Bufferalo@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
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