



Town of Gates

Information Technology

Report of Examination

Period Covered:

January 1, 2011 — April 2, 2012

2012M-169



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
Information System Controls	5
Recommendations	8
APPENDIX A Response From Local Officials	9
APPENDIX B Audit Methodology and Standards	11
APPENDIX C How to Obtain Additional Copies of the Report	12
APPENDIX D Local Regional Office Listing	13

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

November 2012

Dear Town 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 Town Board 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 Town of Gates, 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 Town of Gates (Town) is located in Monroe County with a population of 29,000 residents. The Town is governed by a Town Board (Board) comprising the elected Town Supervisor (Supervisor) and four elected councilpersons. The Board is the legislative body responsible for managing and controlling Town operations. The Supervisor, who serves as the chief financial officer, is responsible, along with other administrative staff, for the day-to-day management of the Town under the direction of the Board. The Town provides various services to its residents including police, highway, library, recreation and parks, and general governmental services. The Town's appropriations for the 2012 fiscal year were approximately \$15 million.

The Town has 85 computers (81 desktops and four laptops) and five physical servers. Four of these servers are at the Town Hall and one is at the library. The Finance Director (Director) is responsible for overseeing the information technology (IT) vendor hired by the Town to manage its IT system. The Director reports to the Supervisor and Board in this capacity. Town officials rely on the IT system and electronic data for making financial decisions, processing transactions, keeping records, and reporting to State and Federal agencies. The Town switched its in-house IT functions over to an external IT vendor on October 4, 2011.

In February 2011, the Town experienced a disruption in services due to the failure of two servers. This equipment failure interrupted operations from one to six days in various departments. In response to the server failures, Town officials developed an IT disaster recovery plan which was completed in January 2012.

Objective

The objective of our audit was to assess the adequacy of the Town's policies and procedures over IT and evaluate the Town's capabilities to restore business processes in the event of an IT system failure. Our audit addressed the following related question:

- Has the Board adopted adequate policies and procedures over IT, including a comprehensive disaster recovery plan (DRP)?

Scope and Methodology

We assessed the Town's IT policies and procedures and DRP for the period January 1, 2011 to April 2, 2012.

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 Town officials and their comments, which appear in Appendix A, have been considered in preparing this report. Town officials generally agree with our recommendations and indicated that they plan 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 Town Clerk's office.

Information Technology

The Town's IT system is a valuable and essential part of operations used for communicating, processing and storing data, and reporting to the Board as well as to various State agencies. If the IT system fails, the resulting problems could range from inconvenient to severe; even small disruptions in electronic data systems can require extensive effort to evaluate and repair. The Board is responsible for creating an appropriate internal control environment over the IT system, including policies and procedures for acceptable computer use, data security, user access, and disaster recovery.

The Board did not adopt IT policies that address topics including personal computer use, password security, and access to sensitive information, nor did the Town have a comprehensive disaster recovery plan (DRP) for resuming critical operations in the event of a system failure. As a result, when a system failure occurred in February 2011, the Town was not prepared and various departmental functions were interrupted from one to six days. Town officials subsequently developed a DRP, completed in January 2012, which we decided to evaluate for effectiveness in the event of any future disruptions. We found that, while the Town still needs to develop and adopt computer policies, its DRP contains all the elements of a comprehensive plan to restore critical services in a timely manner and at minimal cost.

Information System Controls

There are a number of information system controls that can be put in place to safeguard Town resources. The Board can implement a comprehensive set of computer policies that define computer use to assist individuals with recognizing information technology security concerns and then respond appropriately. Other system controls include developing and communicating disaster recovery plans to key Town personnel to ensure they are aware of their responsibilities in preventing, mitigating, and responding to emergency situations. Finally, comprehensive disaster prevention and recovery planning must include provisions for financing any related costs.

Computer Policies – The Board should provide oversight and leadership by establishing computer policies that take into account people, processes, and technology, and communicate the policies throughout the organization. Computer policies define appropriate user behavior and describe the tools and procedures needed to protect data and information systems. Common IT policies address Internet, email, and personal computer use; use of and access to personal, private, and sensitive information; password security; wireless access security; mobile computing and storage devices; and online

banking. In addition, Technology Law Section 208 requires the Town to establish an information breach notification policy detailing how the Town would notify New York State residents whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization.

At the time of our audit, the Town had no written computer policies to address these or any other IT issues. However, we did identify some mitigating controls. For example, Town officials have implemented procedures using application controls in the Town's software to ensure the use of passwords and to provide wireless security. In addition, the Town has procedures in place with its banking institutions to provide controls for online banking.

While computer policies do not guarantee the safety of the Town's computer system or electronic information, the lack of policies significantly increases the risk that data, hardware, and software systems may be lost or damaged by inappropriate access and use. Without comprehensive policies that explicitly convey the appropriate use of the Town's computer equipment, Town officials cannot ensure that Town employees are aware of their responsibilities and there are no consistent standards for which these users are held accountable. In addition, the lack of policies increases the risk of inappropriate computer use (either intentional or accidental) that could potentially expose the Town to virus attacks or compromise computer systems. Without an information breach notification policy, in the event that private information is compromised, Town officials and employees may not be prepared to notify affected individuals.

Disaster Recovery Plan – Disaster recovery planning is the process of preparing for recovery or continuation of technology infrastructure critical to an organization after a disaster. A DRP is the written document identifying and describing how organizations plan to prevent loss of computer equipment and data, and the procedures for recovery in the event of an actual disaster. An effective DRP is designed to quickly and completely reestablish a system or service following a service interruption or disaster, with minimal costs to the organization. The negative impacts of unpreparedness include extended downtime, unavailability of critical services, lost revenue, and loss of public trust. For these reasons, it is critical that organizations limit downtime by developing a comprehensive DRP and implementing effective disaster recovery procedures quickly when an incident occurs.

The importance of having a well designed DRP was underscored in February 2011 when the hard drives in two of the Town's servers failed causing the servers to crash. Town officials had recognized the

need for a DRP and were in the process of developing one; however, they had nothing formally adopted at the time of the crash and were unprepared when the servers crashed and disrupted department operations for up to six days.¹ For example, the police had to book arrestees at a neighboring municipality, and the Justice Court was unable to access its system to process tickets and fulfill other Court responsibilities. In addition, four of the seven Town departments reported email access being inconsistent.

In the year following the server crashes, the Town developed and adopted an appropriate DRP. Our review of the Town's DRP found it to contain all five key elements of a comprehensive DRP² as follows:

- Key individuals and responsibilities are identified and assigned.
- Regular system backups are performed, including applications as well as data, and the backup media is maintained in safe, off-site locations.
- Secondary locations have been identified along with necessary equipment (hardware, software, and peripherals inventory) and access to the off-site backups.
- Disaster recovery procedures are in place to address emergency response, backup operations, and recovery action.
- Procedures are in place for periodic review and testing of the DRP.

Town officials used the server crash as an opportunity to develop a DRP that is not only comprehensive but, in the event of a future disaster, should provide for a timely recovery at minimal costs.

Disaster Recovery Resources – An additional consideration in developing a DRP is ensuring sufficient funds are available to implement the DRP in the event a disaster occurs. Therefore, effective disaster recovery planning must include various financial considerations. There are costs associated with preventive measures identified during planning, as well as different costs for implementing various recovery scenarios. Risk assessment can help estimate the cost of options and decide on an optimal strategy. Part of this

¹ At the time of the crash, the Town was preparing to transition to new servers, which minimized disruption. Otherwise, this situation could have resulted in an extended period of disruption.

² For an explanation of how we determined these criteria, see Appendix B – Audit Methodology and Standards.

assessment is determining whether the consequences of a loss of computer-related resources in a particular function are sufficiently high to warrant the cost of various recovery strategies. Once these various costs are identified and strategies are selected, the Town should lay out plans for how to fund them.

We evaluated whether the Town identified and planned for adequate financial resources to provide reasonable assurance that essential business operations would be efficiently recovered. The Town's current service agreement with its IT vendor includes most DRP services without additional costs to the Town.³ Further, to prevent aged equipment failures⁴ like the one that caused the two servers to crash in February 2011, Town officials adopted a capital plan covering the 2012 through 2016 fiscal years. The capital plan includes \$20,000 a year for the purchase of computer and server equipment to keep the current IT system up-to-date. Consequently, it appears the Town has identified and planned for adequate financial resources during its DRP development process.

Recommendations

1. The Board should adopt comprehensive written IT policies and procedures, review them periodically, and update them as needed.
2. Town officials should continue to review, update, and test the DRP on a periodic basis. This evaluation should include the adequacy of the financial resources provided.

³ The DRP does identify a minimal additional outlay: a \$1,000 fee plus the cost of transport for a replacement network-attached storage device loaded with a complete backup. This would serve as a replacement server for the Town during disaster recovery, as in the situation that resulted from the complete loss of the Town Hall's server facilities.

⁴ The Town's previous servers were eight years old when the hard drives crashed.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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



TOWN OF GATES

1605 BUFFALO ROAD
GATES, NEW YORK 14624
PHONE (585) 247-6100 • FAX (585) 247-0017

MARK W. ASSINI
SUPERVISOR

TOWN COUNCIL

FRANK X. ALLKOEFER
CHRISTOPHER B. DIPONZIO
ELAINE P. TETTE
RICHARD A. WARNER

The Town of Gates would like to thank the Comptroller's office for reviewing our Disaster Recovery Plan (DRP). We are pleased that the plan established by the town meets all the criteria of an effective and well designed DRP. Our plan assures town data will be protected and business continuity will be maintained in a disaster scenario.

In April 2012 the town passed and implemented a Breach Notification Policy which identifies the steps that town employees must take when personal information held by the town has been comprised by a security breach. We are proud that Gates was among the first towns in this county to pass such a policy.

Finally, we agree that the town should establish a Policy for Acceptable Internet and Computer Use. We do have elements of this policy currently in place. To outline what is in place now;

1. The town is using Internet content filtering hardware which limits where an employee can go on the town network as well as the internet. Access for an employee to any network or internet location has been set up on a need only basis by job function.
2. Our ethics code prohibits personal use of town assets. This code is fortified by our annual ethics training course for employees where we identify what is an acceptable use of computers and what is unacceptable. This includes internet usage.

Consolidating the various pieces into one policy document is appropriate and wise. I plan to submit a Policy for Acceptable Internet and Computer Use to the Town Board for review and approval at the December 2012 Board meeting. This document will be distributed to the employees, placed in the employee handbook and reviewed at our annual ethics training class. The Gates Town Board will review both our DRP and Acceptable Internet & Computer Use Policy on a regular basis and change them as needed.

My thanks once again to the staff from the Comptroller's office which was both courteous and professional. We are grateful for their help.

Respectfully,

Mark Assini
Gates Town Supervisor

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations and performing a preliminary review concerning disaster recovery and business continuity planning. We obtained a high-level understanding of the IT environment and conducted a high-level risk assessment pertaining to the IT environment. During the initial assessment, we interviewed appropriate Town officials and reviewed pertinent documents, such as Town policies and procedures. Upon completion of our pre-audit work, we determined the scope and objectives of the audit. We selected disaster recovery and information technology policies and procedures for further testing.

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

- We reviewed appropriate policies and procedures.
- We interviewed appropriate Town officials to obtain additional information regarding the procedures and practices surrounding information technology.
- We compared internal guidance on recommended IT policies to the Town's written policies.
- We interviewed appropriate Town officials and the IT vendor regarding the Town's disaster recovery planning process.
- We reviewed recommendations from four independent IT expert resources as well as interviewed internal IT experts to identify key elements of a DRP. We reviewed the elements identified by the experts with Town officials and compared these to the Town's DRP.
- We reviewed appropriate documentation supporting assertions made by Town officials and the IT vendor regarding the Town's disaster recovery planning process.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

Christopher Ellis, 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 AND REGIONAL PROJECTS

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