



NEW YORK STATE BRIDGE AUTHORITY

P.O. Box 1010, Highland, New York 12528 P: (845) 691-7245 F: (845) 691-3560

ANDREW M. CUOMO, *Governor*

JOSEPH RUGGIERO, *Executive Director*

BOARD

RICHARD A. GERENTINE
Chairman

JOSEPH RAMAGLIA
Vice Chairman

RODERICK O. DRESSEL
C. VANE LASHUA

ROGER P. HIGGINS

MEMORANDUM

To: Joe Ruggiero
From: Brian Bushek
Date: March 7, 2014
Subject: 2013 INTERNAL AUDITORS' REPORT

In 2011, the Authority contracted the firm Tronconi, Segarra & Associates to assist in compliance with the requirements of Public Authorities Law associated with internal controls. In March 2011, the requirement to file form New York State Budget Policy & Reporting Manual B-350 was eliminated for Public Authorities, but all of the requirements of the Internal Control Act remained. The Authority is required to complete an annual assessment of the effectiveness of the internal control structures and procedures. The assessment must be posted on the Authority's website for a period of two years.

The attached annual assessment report prepared by Tronconi, Segarra & Associates is presented to the Audit Committee for information purposes only. No action by the Board is required.

The report covers the four areas that were outlined in the previously provided 3 year audit program. Specifically: Toll Collection & Revenues (TCR), Contract Coordination & Supervision (CCS), Financial Reporting (FR), and Information Technology (IT).

The Authority continues to demonstrate strong controls and is pleased to note that for these four areas the Auditor identified only the IT area with three recommendations to strengthen the Authority's controls and risk exposure. It should be noted that this is the first time the Internal Audit function has reviewed the IT function. None of the recommendations were considered "urgent." Due to the nature of the recommendations the implementation of measures to address each of these items has been or will be quickly implemented.

The individual recommendations and action are detailed below.

Information Technology (IT)

1. Authority policies and procedures provide guidelines for creating strong passwords. However, in practice, the IT Department does not require passwords be case sensitive nor contain special characters.

Authority policies had recommended a greater level of password complexity than the complexity codified (required) of users in Authority systems. The existing complexity

RIP VAN WINKLE
P.O. Box 286
Catskill, NY 12414
(518) 943-2360

KINGSTON-RHINECLIFF
P.O. Box 1400
Kingston, NY 12402
(845) 336-8181

MID-HUDSON
P.O. Box 1010
Highland, NY 12528
(845) 691-7221

NEWBURGH-BEACON
P.O. Box 28
Beacon, NY 12508
(845) 831-3700

BEAR MOUNTAIN
P.O. Box 323
Ft. Montgomery, NY 10922
(845) 446-4721

codified baseline requirements specified by NY State, but did not require all of the complexity recommended in its guidelines. Based on the recommendation the Authority will now enhance the complexity password requirements in its systems as defined in the policies procedures. Responsibility to implement this recommendation resides with Greg Herd.

2. The server room is not equipped with an automatic fire suppression system.

The Authority has evaluated the risk associated with the server room and designed systems in a decentralized manner with processes to create frequent offsite backups as part of its disaster recovery planning. The Authority recognizes that some risk exposure remains in the server room even after risk mitigation efforts have been taken. After a cost/benefit review of available options, the Authority has initiated a process to procure the installation of a fire suppression system in the server room. A purchase order was issued in February to address this item for \$11,801. Responsibility to implement this recommendation resides with Bill Moreau.

3. No surveys are provided to users at the completion of a work ticket. The NYSBA's IT Department does not provide surveys to solicit feedback from users once a work ticket is completed.

The Authority has reviewed this recommendation and evaluated the capability of its existing help desk ticket system. The current software does not provide the capability to include a feedback survey. The Authority utilizes a free solution for its helpdesk system that is not feasible to invest in an upgrade to allow this capability. Given the Authority recognizes the benefits of the capability and the largest number of help desk tickets are produced by a handful of frequent users, we will research viable solutions. Responsibility to develop and implement a solution resides with Francine Byrne and Greg Herd.

The Authority will review all remediation efforts and report back to the Audit Committee during or before the June 2014 Board meeting.

New York State Bridge Authority

**Risk Assessment
Recommendations and Findings
For 2013**

New York State Bridge Authority
Risk Assessment,
Recommendations and Findings
For 2013

Table of Contents

	<u>Page</u>
Transmittal Letter	
Risk Assessment	
Overview.....	1
Risk Management Tolerance Model.....	3
Risk Assessment Matrix.....	4
Internal Control Recommendations	
Overview.....	5
Toll Collections & Revenues.....	6
Contract Coordination & Supervision.....	6
Financial Reporting.....	6
Information Technology.....	6

Mr. Roger Higgins
Audit Committee Chairman
New York State Bridge Authority
Mid-Hudson Bridge Toll Plaza – State Routes 44/55
P.O. Box 1010
Highland, New York 12528

Dear Mr. Higgins,

We are pleased to report on our annual assessment of the internal controls of the New York State Bridge Authority (the “Authority”). The purpose of our engagement was to assist the Authority in achieving compliance with the applicable provisions of the *Public Authorities Accountability Act of 2005* as amended by the *Public Authorities Reform Act of 2009* (the “Act”). Among other requirements, Public Authorities Law requires all public authorities to complete an annual assessment of the effectiveness of their internal control structure and procedures within ninety (90) days after the end of its fiscal year. Additionally, State authorities with a majority of the members appointed by the Governor must establish and maintain a system of internal control and a program of internal control review.

The importance of an adequate system of internal control is to promote effective and efficient operations so as to help the Authority carry out its mission; to provide reasonable, but not absolute, assurance that assets are safeguarded against inappropriate or unauthorized use; to promote the accuracy and reliability of accounting data and financial reporting to ensure transactions are executed in accordance with management’s authorization and recorded properly in accounting records; to encourage adherence to management’s policies and procedures for conducting programs and operations; and to ensure compliance with applicable laws and regulations. Furthermore, a successful system of internal control includes performing an annual assessment to identify potential weaknesses in policies and procedures and to implement corrective actions.

This report contains the results of our procedures performed on the following major business functions (cycles):

- Toll Collection & Revenues
- Contract Coordination & Supervision
- Financial Reporting
- Information Technology

Internal control testing was performed through tailored procedures designed based on our understanding of the Authority’s relevant policies and procedures in effect for the aforementioned cycles between January 1, 2013 and December 31, 2013.

The Authority’s risks are the risks that an action or event will adversely affect the Authority’s ability to successfully achieve its objectives. The Risk Assessment section of the report analyzes the significant risk findings that were identified during our assessment.

For purposes of complying with the Act, an internal control assessment is an annual evaluation performed by management (or its designee) to determine the effectiveness of the Authority's internal control system. We have evaluated the Authority's current internal controls within the cycles listed above and have provided our risk assessment and a set of recommendations for strengthening controls and reducing identified risks.

As previously discussed, the purpose of our engagement was to assist the Authority in achieving compliance with the Act through the performance of an annual assessment of the effectiveness of its internal control structure and procedures. However, it is ultimately management's responsibility to assess the adequacy of the Authority's internal control structure and the adequacy of its procedures. In performing our assessment, we relied on the accuracy and reliability of information provided by Authority personnel. We have not audited, examined, or reviewed the information, and express no assurance thereon.

The accompanying comments and recommendations are intended solely for the information and use of the Authority, its department heads, and others within the Authority, and should not be used for any other purpose.

We appreciate the opportunity to serve you and thank the employees of the Authority for their cooperation. We have already discussed many of these comments and suggestions with various Authority personnel, and we will be pleased to discuss them in further detail at your convenience. Through our ongoing involvement with you as a client and our knowledge of your processes, we would be pleased to perform any additional studies of these matters, or to assist you in implementing the recommendations.

Traxson Segura & Associates LLP

December 3, 2013

Risk Assessment

New York State Bridge Authority

Risk Assessment

Overview

The Authority's risks are the risks that an action or event will adversely affect the Authority's ability to successfully achieve its objectives. During our engagement we became aware of various sources of risk that impact the Authority. We evaluated these risks by using two distinct assessments of impact and likelihood. A simple rating scale has been developed for this purpose. The rating scale ranges from minor to significant impact, and low to high likelihood, using a 3-point scale.

Impact refers to the extent of the consequences or implications if the risk does occur. To assess impact, we have determined how much of an impact the risk has if it does occur:

- A minor impact suggests that the risk would not have important implications to the Authority.
- A moderate impact suggests that the risk could have implications affecting the Authority's ability to succeed.
- A significant impact suggests that the risk would have important implications to the Authority.

Likelihood refers to the probability that the risk may occur given the current context of the Authority. To assess likelihood, we have determined how likely it is that the risk will occur in the future, given what is currently done to manage said risk:

- A low likelihood suggests that the risk is unlikely to occur, given its nature and current risk management practices in place.
- A medium likelihood of occurrence suggests that the risk has a moderate probability of occurrence.
- A high likelihood of occurrence suggests that the risk is likely to occur, despite the current risk management practices in place.

The Risk Management Tolerance Model and the Risk Assessment Matrix that follows summarizes these risks and assesses their impact and likelihood.

New York State Bridge Authority

Risk Assessment (continued)

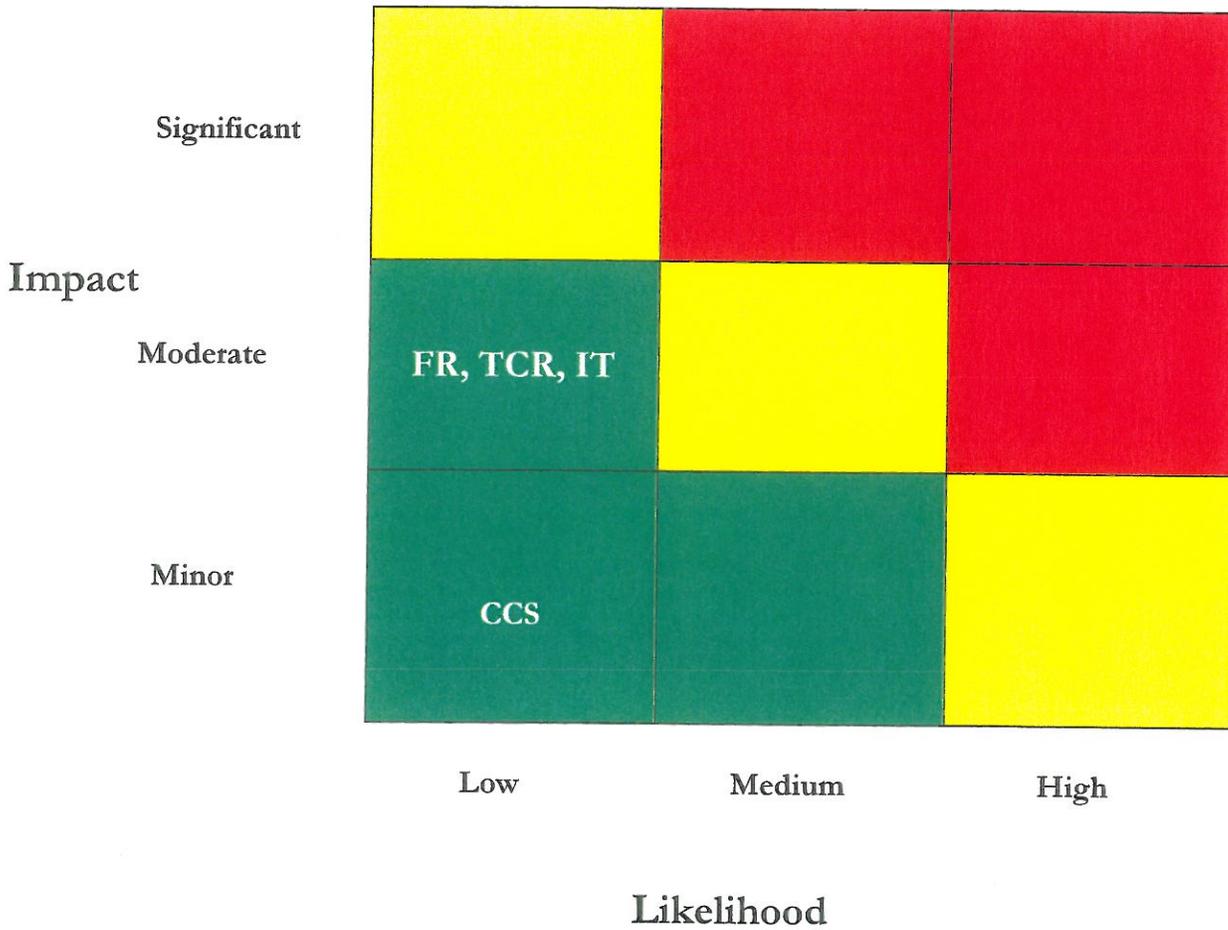
Cycles plotted in the red sections of the model are considered to be high risk and, as such, the related deficiencies should be given urgent attention in terms of priority. Cycles plotted in the yellow sections are considered to have moderate risk, are considered to be important, and should be given second priority after the high risk cycles. Cycles plotted in the green section of the model are considered least risky and remediation efforts to address deficiencies in these cycles would be expected to be addressed during routine operations of the Authority.

We have developed the risk assessment around significant transaction cycles as a means by which the associated risks can be easily understood and managed. The Internal Control Recommendations section of this report presents recommendations with more detail information regarding criticality and implementation timeliness. The cycles or areas that have been evaluated are:

- Toll Collection & Revenues (TCR)
- Contract Coordination & Supervision (CCS)
- Financial Reporting (FR)
- Information Technology (IT)

New York State Bridge Authority
Risk Assessment (continued)

Risk Management Tolerance Model



New York State Bridge Authority
Risk Assessment (continued)

Risk Assessment Matrix

<u>Cycle</u>	<u>Risk Assessment Based on Procedures Performed</u>	<u>Impact*</u>	<u>Likelihood*</u>
TCR	We noted minor overall risk in the Toll Collection & Revenues cycle. There were no control deficiencies noted at the time of our analysis.	Moderate	Low
CCS	We noted minor overall risk in the Contract Coordination and Supervision cycle. There were no control deficiencies noted at the time of our analysis.	Minor	Low
FR	We noted minor overall risk in the Financial Reporting cycle. There were no control deficiencies noted at the time of our analysis.	Moderate	Low
IT	We noted moderate overall risk in the Information Technology cycle. Certain IT Controls should be strengthened.	Moderate	Low

*The impact and likelihood noted above relates to the overall risk of the cycles and does not correlate to specific findings noted on the following pages.

Internal Control Recommendations

New York State Bridge Authority

Internal Control Recommendations

Overview

Internal control recommendations represent those areas that afford department heads of the Authority the opportunity to improve financial reporting and internal controls, to better safeguard Authority assets, and/or to more efficiently or accurately record, summarize, and report financial transactions and information. They also represent those areas that may improve efficiency of operations and accounting functions, potentially resulting in cost savings.

We have provided a criticality rating and an implementation timeline for each internal control recommendation and business opportunity. Criticality ratings have been categorized as either routine, important, or urgent, and are intended to assist the Authority in determining priority during remediation. The implementation timelines considered were short-term and long-term, reflecting the effort and time required to implement the applicable recommendation while factoring in the criticality assigned thereto.

As a result of our procedures performed, there were 3 total recommendations:

<u>Internal Control Area</u>	<u>Recommendations</u>	<u>Criticality</u>			<u>Timeline</u>	
		<u>Routine</u>	<u>Important</u>	<u>Urgent</u>	<u>Short-Term</u>	<u>Long-Term</u>
Toll Collection & Revenues (TCR)	-	-	-	-	-	-
Contract Coordination & Supervision (CCS)	-	-	-	-	-	-
Financial Reporting (FR)	-	-	-	-	-	-
Information Technology (IT)	3	1	2	-	3	-
Total	3	1	2	-	3	-

Timeline – each of the detail findings includes a timeline reference of either “short-term” or “long-term.” Short-term refers to a finding that we believe can be corrected within one year. Long-term refers to a finding that may require changes to organization, systems, and/or procedures that may require over one year to effectuate change.

New York State Bridge Authority
Internal Control Recommendations (continued)

Toll Collection & Revenues (TCR)

There were no findings as a result of our procedures.

Contract Coordination & Supervision (CCS)

There were no findings as a result of our procedures.

Financial Reporting (FR)

There were no findings as a result of our procedures.

Information Technology (IT)

Recommendation #IT1

Criticality: Important

Timeline: Short-Term

Finding: The Authority's written Policies and Procedures provide guidelines on creating strong passwords. However, in practice, the IT Department does not require passwords to be case sensitive nor contain special characters. The password has to be at least 8 alphanumeric characters. The Authority does not enforce the written password policy, which requires strong passwords to be case sensitive and contain at least one special character.

Background: Passwords should contain complexity requirements. They should be at least eight characters and contain an uppercase, lowercase, numeric, and special character. They should not include the use of names or words that can be easily guessed or identified using a password-cracking mechanism, should be required to be changed periodically (every 30-90 days), and should not allow the last six passwords to be reused.

Rationale:

Impact: *Moderate* - Unauthorized access to the NYSBA network could obstruct day-to-day operations based on the purpose of the access.

Likelihood: *Low* - The NYSBA still requires moderately strong passwords that contain at least 8 alphanumeric characters.

Recommendation: The NYSBA should enforce its password policy by requiring all employee passwords to contain upper and lower case letters, numbers, and special characters.

New York State Bridge Authority
Internal Control Recommendations (continued)

Recommendation #IT2

Criticality: Important

Timeline: Short-Term

Finding: The server room is not equipped with an automatic fire suppression system. It does have a small fire extinguisher.

Background: Automatic and manual fire-suppression systems should be installed in the server rooms and wiring closets and periodically inspected, tested and maintained internally or by a qualified third-party in accordance with the National Fire Protection Association requirements as listed at <http://www.nfpa.org/codes-and-standards/document-information-pages>. In addition, IT administration should be trained in how to use the fire-suppression system.

Rationale:

Impact - Significant - If a fire were to breakout in the server room, the small fire extinguisher maintained would not be sufficient to limit loss to the equipment.

Likelihood - Low - The server room is maintained in a properly climate controlled environment, and all electronic equipment is plugged into surge protectors.

Recommendation: The NYSBA should consider installing an automatic fire suppression system within the server room to limit equipment loss due to fire.

Recommendation #IT3

Criticality: Routine

Timeline: Short-Term

Finding: No surveys are provided to users at the completion of a work ticket. The NYSBA's IT Department does not provide surveys to solicit feedback from users once a work ticket is completed.

Background: IT Help Desk surveys are not provided to end users to solicit feedback from them.

Rationale:

Impact - Moderate - The use of the software is currently efficient. Surveys may provide additional information on areas for general improvement within the help desk process.

Likelihood - Low - We are not aware of any risks caused by the Help Desk process.

Recommendation: The NYSBA should research if a survey add-on function is available within the Spice Works Help Desk module. Ideally, a survey should be automatically sent to a user once a ticket is closed.