

April 2, 2013

Irene Lynch-Larivee, Finance Director
Town of Nantucket
16 Broad Street
Nantucket, MA 02554

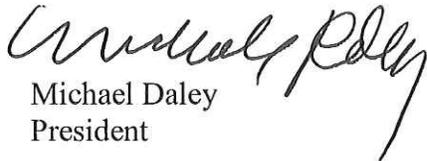
Dear Ms. Lynch-Larivee:

Financial Advisory Associates, Inc. has completed the first annual fraud risk assessment for the town of Nantucket. You will find the report enclosed.

Thank you for the opportunity to be of service to the town. We look forward to the next phase of this project.

Sincerely yours,

FINANCIAL ADVISORY ASSOCIATES, INC.



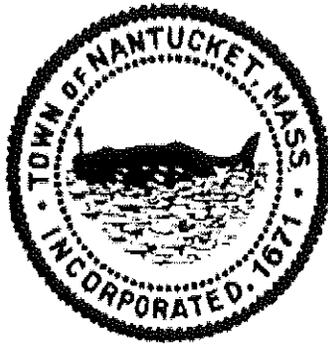
Michael Daley
President

Enclosure

A Fraud Risk Assessment

For

The Town of Nantucket



Prepared by
Financial Advisory Associates, Inc.
258 Main Street, Suite A2
Buzzards Bay, MA 02532
February 15, 2013

FAA
Financial Advisory Associates, Inc.

February 15, 2013

Irene Lynch-Larivee, Finance Director
Town of Nantucket
16 Broad Street
Nantucket, MA 02554

Dear Ms. Lynch-Larivee:

Financial Advisory Associates, Inc. entered into an agreement with the town of Nantucket to assist the town with the commencement of an annual fraud risk assessment.

During fiscal year 2013, at your direction, we have assisted your department to conduct a fraud risk assessment within the town's Department of Public Works, Human Resources Department and Memorial Airport.

Enclosed within please find the summary report and the detailed assessment documentation we have prepared.

We wish to thank you and your staff for the enthusiastic support we have been provided during our work. We also wish to thank the three town departments for all the efforts they made to help make this a quality review process.

Sincerely yours,
Financial Advisory Associates, Inc.

Michael Daley
President

258 Main Street, Suite A2
Buzzards Bay, MA 02532
Phone 508.759.0700 Fax 508.759.6418 email: info@faa-inc.com

Introduction

Introduction

The Sarbanes-Oxley Act (SOX) of 2002 requires public entities, among other things, to evaluate the sufficiency of controls in place to prevent and detect fraud within the organization. Specific to fraud, Section 404 of SOX requires that each corporate organization have a documented and on-going process to identify, assess and evaluate fraud risks related to internal control over financial reporting ("fraud risks"). Section 404 also clearly directs responsibility for the establishment and monitoring of such a process to the entity's Management, the organization's Governance Board and their Audit Committee.

This document provides an overview of the process Nantucket's management undertook to satisfy the requirements of SOX Section 404 related to the consideration and evaluation of fraud risk as it pertains to internal control over financial reporting. Management understands that this process is not a one-time event and they must routinely update their internal assessment of such fraud risks facing the Town annually at a minimum. The results of this assessment provide a point in time snapshot of fraud risks within three departments and their potential impact to the overall organization.

Risk Assessment Scope

In order to clearly define the scope of this risk assessment, the definitions of key terms utilized throughout the course of this exercise are provided below.

Nantucket defines fraud as any intentional act that is committed to secure an unfair or unlawful gain. The four categories of fraud related to internal control over financial reporting considered by management in this assessment are:

- **Fraudulent Financial Reporting** – Most fraudulent financial reporting schemes involve earnings management, arising from improper revenue recognition, and overstatement of assets or understatement of liabilities.
- **Misappropriation of Assets** – This category involves external and internal schemes, such as embezzlement, payroll fraud and theft.
- **Expenditures and liabilities for improper purposes** – This category refers to commercial and public bribery, as well as other improper payment schemes.
- **Fraudulently obtained revenue and assets, costs and expense avoided** – This category refers to schemes where an entity commits a fraud against its employees or third parties, or when an entity improperly avoids an expense, such as tax fraud.

Additionally, it is important to note that various fraud schemes/scenarios can be perpetuated at many different locations or levels within an organization. For the purpose of this assessment, Nantucket considers fraud that can occur at three levels:

- Account-level
- Process-level
- Entity-level

Account-level and process-level fraud risks are defined as risks that are contained to a specific account or process, and their impacts generally do not have a significant impact to the organization as a whole. As such, these risks will be identified and evaluated as part of the process documentation created for each relevant business area. Within the control documentation for each business process, specific, relevant fraud risks will be identified, and corresponding controls will be linked to these risks and tested based upon their significance.

Management defines entity-level fraud risks as those schemes and scenarios that may be undertaken by employees, agents, vendors or other parties that could have a material impact to the organization, either directly through financial statement impact or through other indirect means (e.g., reputation deterioration, etc.). Entity-level fraud risks will be considered separately. FAA, Inc prepared a risk and control matrix of entity-level fraud risks and associated controls for the organization. The presentation of these risks and controls will be similar to the control documentation prepared for individual business processes. The remainder of this document details the process by which entity-level fraud risks were identified and assessed throughout the organization.

Fraud Risk Identification

In order to conclude upon whether management has established and implemented an effective antifraud program, an organization must determine what potential vulnerabilities exist with regard to fraud perpetrated within the company and against the company. The Public Companies Audit Oversight Board (PCAOB) and the Security and Exchange Commission (SEC) provide guidance that each public entity should consider potential fraud schemes and scenarios that could be perpetuated by an organization and against an organization. Both the PCAOB and the SEC also advise corporate organizations to pay special attention to the risk of management override of controls that could result in fraudulent activity.

FAA, Inc developed the initial population of potential fraud schemes/scenarios using a number of documents and tools to assist in this process. Those tools included:

- Development and use of initial internal audit process-level risk assessment forms
- Fraud training materials obtained through various seminars and outside vendors
- External literature on the topic of fraud

In addition to these tools, FAA's significant knowledge of the town's operations coupled with the experience and expertise of the internal finance team in auditing each department was key to developing a comprehensive population of potential fraud schemes/scenarios. FAA formally defined each fraud scenario that was relevant to the town to ensure a common understanding of each risk by all relevant town personnel. The potential fraud schemes and scenarios should be considered across the entire organization and are broken down into functional areas of the business.

After completing a first draft of the population of potential fraud schemes/scenarios, the results were presented to the town's finance team for review. Feedback was gathered and incorporated to provide a comprehensive list of potential fraud risks throughout each department evaluated. Additionally, FAA met with various senior management personnel to discuss the universe of fraud scenarios in greater detail. Feedback gathered from these meetings was incorporated as necessary to add clarity to definitions and ensure agreement as to the completeness of the population of risks identified.

Risk Rating

Once the population of fraud schemes and scenarios was compiled, FAA, Inc preliminarily ranked the fraud exposure of each functional area of the Town evaluated. A rating of High, Moderate or Low was assigned to each of four Risk Categories: (1) General, (2) Other Reviews and Audits, (3) Specific Financial Risk Areas and (4) Systems. These ratings represent the overall likelihood and potential magnitude of all potential fraud schemes/scenarios that were identified for each functional area.

The initial risk rating exercise revealed, not unexpectedly, that all three functional areas of the town we reviewed did possess at least a moderate inherent risk of fraud of some manner. These results were presented to the town's management for review.

As a result of this rating exercise, each of the three business areas presented unique fraud schemes/scenarios, compelling management to evaluate the sufficiency of controls in place to prevent and/or detect fraudulent activity from occurring. In order to focus our analysis and evaluation of anti-fraud controls; FAA, Inc rated each individual scheme/scenario using the same criteria applied to each functional area.

Risk and Control Analysis

The evaluation of antifraud controls will closely follow the Section 404 evaluation of financial reporting controls within the town. This evaluation process is two-part: (1) evaluating the design of controls and (2) subsequently evaluating each control's operating effectiveness.

Design Evaluation

The Finance Department is responsible for working with department heads to identify controls that are designed to prevent potential fraud schemes/scenarios from occurring and/or detect the occurrence of such activities. Each scheme/scenario identified by management will be assessed individually. The Finance Department is responsible for assisting departmental management in its evaluation of determining whether an appropriate mix of preventive and detective controls are in place, based upon the nature, likelihood of occurrence and potential magnitude of each individual scheme/scenario.

After creating an inventory of all controls in place, the Finance Department presents the control documentation and gap analysis to the relevant Department Heads for review and approval. The Finance Department and the Department Heads work together to develop remediation plans for any control design gaps identified.

Effectiveness Evaluation

The Finance Department is also responsible for ensuring that antifraud controls are operating as designed. Following the same procedures utilized for assessing the operating effectiveness of other town controls within the scope of Section 404, the Finance Department will develop and execute test plans to ascertain whether controls designed to prevent or detect fraud operate as intended. As with tests of other controls, the Finance Department will determine the appropriate mix of test procedures (i.e., re-performance, inspection, observation or inquiry) to provide sufficient evidence as to whether each control is operating as intended.

Presentation of Completed Anti-Fraud Program Analysis

In conjunction with provisions set forth in the Sarbanes-Oxley Act of 2002, the results of the fraud risk assessment will be presented to the town's Governing Board. The Board is ultimately responsible to perform adequate oversight over the conclusions management derives from its evaluation of its anti-fraud program.

For fiscal year 2013, the results of the fraud risk assessment will be presented through the Audit Committee to the town's Governing Board members. Minutes from these meetings will be prepared and will then provide additional details of the presentation and discussion of the anti-fraud program within the Town.

Entity Level Findings

As a result of the town's initial fraud risk assessment we have the following findings to present.

1. Develop a town-wide Fraud Mitigation and Detection Policy.

The Town of Nantucket does not presently have a formal policy relating to the prevention and detection of fraudulent actions. Employees and other town officials do not receive any formal training or education regarding anti-fraudulent behavior. There is no "whistleblower" protection presently provided to employees. There is no "hotline" or other highly visible means made available by the town for their employees or other internal or external individuals to report perceived acts of fraud.

We recommend that the town develop and implement a formal Fraud Detection and Mitigation Policy and Program.

2. Review and solidify town-wide payroll review, approval and oath procedures.

The state uses MGL C41, §41 as a municipal payroll internal control. This provision of the law establishes that appointing authority or department head "sworn" payroll signoffs are mandatory. All alternate payroll signers must be designated by the appointing authority or department head and approved by the Board of Selectmen. Multi-body appointing authorities may delegate a single member to sign payrolls.

We recommend that the town review, update and validate that payroll approvals all made only by authorized departmental payroll signatories.

3. Review and inventory town-wide fine art collection.

We noted that some town-owned fine art was on display and thus in various department's care and custody. We were not engaged to validate the control and security of the town's collection of artifacts. We do believe an internal review of the current town-wide fine art inventory control systems will disclose the current level of value and risk.

We recommend that the town review the current fine arts controls and conduct an inventory of its fine arts collection.

Department of Public Works

FAA, Inc. Risk Assessment Questionnaire

GENERAL RISK ASSESSMENT Risk Assessment Questionnaire - Summary

AGENCY	Town of Nantucket Department of Public Works		
CYCLE	Initial Assessment	SYSTEM	Fraud Risk
PREPARED BY	FAA, Inc	DATE: 09/11/2012	

Given the results of the risk assessment guideline and other factors I have considered, in my opinion, the system being assessed has the following risk to the agency:

	HIGH RISK (41 – 70)	Internal control evaluation required
33 Points =	MEDIUM RISK (18 – 40)	Internal control evaluation recommended on a cyclical basis.
	LOW RISK (0 – 17)	Internal control evaluation not required.

Please read the explanation of each risk category and evaluation factor on the following pages. Then **assign a rating value in the box provided below**. The rating should be from 0 to 5, with 0 being the lowest or no risk and 5 being the highest or maximum risk.

ASSIGNED RISK CATEGORY	EVALUATION FACTOR	NO.	RATING
General	Outside Interest	1	1.00
	Regulatory/Contractual	2	2.00
	Employee Turnover	3	1.00
Other Reviews and Audits	Audit Coverage	4	0.00
	Results of Prior Reviews	5	5.00
Specific Financial Risk Areas	Account Balance Size	6	2.00
	General Fund State	7	3.00
	Federal Assistance Programs	8	3.00
	Cash	9	3.00
	Merchandise	10	5.00
	Fixed Assets	11	3.00
System	Automation	12	3.00
	Decentralization	13	1.00
	Sensitive Data	14	1.00
		TOTAL	33.00

**FAA, Inc. Control Environment
Control Policies and Procedures Questionnaire**

Municipality: Nantucket

Department: Public Works

Fiscal Year: 2013

A. Integrity and Ethical Values

Yes No N/A

1. Does the agency have a code of ethical conduct that has been made available to all employees?
2. Does the code of conduct address policy for potential conflicts of interest?
3. Is there a procedure in place for employees to report fraudulent or dishonest acts?
4. Does Management take appropriate disciplinary action when necessary to enforce the code of conduct?

B. Commitment to Competence

Yes No N/A

5. Does management understand the knowledge and skills required to accomplish tasks?
6. Does the entity provide for applicable training of its employees?
7. Do accounting personnel appear to have sufficient expertise in selecting and applying applicable accounting principles?
8. Do accounting supervisors appear to have sufficient expertise to review accounting transactions for accuracy and compliance with rules and regulations?
9. Are sufficient training opportunities to improve competency and update employees on new policies and procedures available?

C. Management's Philosophy and Operating Style

Yes No N/A

10. Are principal accounting records and accounting employees at all locations under the supervision of the principal accounting officer?
11. Are management and operating decisions determined at appropriate levels?
12. Are policies and procedures consistent with statutory authority?
13. Does management review audit recommendations and take appropriate corrective action?
14. Is the internal control structure supervised and reviewed by management to determine if it is operating as intended?

D. Organizational Structure

Yes No N/A

15. Is there an organization chart clearly defining the lines of management authority and responsibility?
16. Is the organization chart current and accurate?
17. Are policies and procedures for authorizations established at a reasonably high level?
18. Have specific line of authority and responsibility been established to ensure compliance with federal and state laws and regulations?
19. Are all the agency's operations centralized or decentralized?
20. If decentralized, is monitoring of the areas adequate?

E. Assignment of Authority and Responsibility

Yes No N/A

21. Has management provided resources to ensure compliance with grant requirements and federal and state laws?
22. Is management actively involved in supervision of the various functions?
23. Has fiscal authority been formally delegated to specific management personnel?
24. Are responsibilities divided so that no single employee controls all phases of a transaction?

F. Human Resource Policies and Practices

Yes No N/A

25. Are competent personnel recruited?
26. Are accurate, up-to-date-position descriptions available?
27. Are managers and employees held accountable for satisfactory completion of performance elements?
28. Do all supervisors and managers have at least a working knowledge of the State's personnel policies and procedures?
29. Does each supervisor and manager have a copy or access to a copy of the State's personnel policies and procedures?
30. Does management ensure compliance with the department's personnel policies and procedures manual concerning hiring, training, promoting, and compensating employees?
31. Has management established backup plans for sudden or significant changes in personnel?
32. Are supervisors readily available to help personnel with non-routine problems?
33. Are external audits performed on a periodic basis?
34. Are background checks performed on certain people who have access to personal information, positions of accounting and financial oversight, and positions of trust?

**FAA, Inc. Computer Security
Control Policies and Procedures Questionnaire**

Municipality: Nantucket

Department: Public Works

Fiscal Year: 2013

A. Control Activities / Information and Communication:

Yes No N/A

1. Does management determine the type of access a new employee should be given and communicate it to the appropriate personnel?
2. Once roles have been established for a new employee by the appropriate personnel are roles given back to management to confirm that appropriate access was granted?
3. Does management approve all changes made to roles?
4. Are terminated employees removed from the roles on the last day of service?
5. Are responsibilities segregated to assure that no one individual has entry and approval roles?
6. Does every user have a unique user-id/password?
- a. Are user passwords kept secret from other users?
- b. Are user passwords changed periodically?
- c. Are users aware of the confidential nature of their passwords?
7. Does management restrict users' access to the minimum level needed to perform their job?

FAA, Inc. Fraud Risk Assessment Form

Municipality: Town of Nantucket

Department: Department of Public Works

Fiscal Year: 2013

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI-FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Financial Reporting:								
Revenue Recognition:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Expenditures Recognition:	FY Payments Timing	Remote	Significant	Public Works Dept	A/P Processing + Year End Processing	Adequate	N/A	N/A
Balance Sheet/Management Estimates:	Misstated Inventory	Remote	Insignificant	Public Works Dept/Accounting Dept	Manual Inventory Control System	Adequate	Inaccuracy	Automate Inventory Control
	Misstated Compensated Absences	Remote	Insignificant	Public Works Dept/Accounting Dept	MUNIS System + Labor Agreement Maximums	Adequate	Inaccuracy	Periodic Testing By Accounting
Disclosures:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Other Reporting:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

FAA, Inc. Fraud Risk Assessment Form

Municipality: Town of Nantucket

Department: Department of Public Works

Fiscal Year: 2013

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI- FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Misappropriation of Assets:								
Cash/Checks/Credit Cards:								
A. Point of Sales	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
B. Accounts Receivable	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
C. Disbursement/Vendor	False Payments	Remote	Insignificant	Public Works	Vendor Controls Multiple Reviews	Adequate	Management Override	Periodic Testing By Accounting
D. Payroll	Falsified Employee Attendance Reports	Remote	Insignificant	Public Works	Multiple Reviews	Inadequate – See Narrative	Management Override	Periodic Testing By Accounting
E. Other	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Inventory:								
A. Tangible Fuel	Theft/Misuse	Remote	Significant	Public Works	Manual Inventory Control	Adequate	Management Override	Automate Fuel Inventory Control
Equipment/Small Tools	Theft/Misuse	Remote	Insignificant	Public Works	Manual Inventory Control	Adequate	Management Override	Automate Inventory Control
Materials	Theft/Misuse	Remote	Insignificant	Public Works	Manual Inventory Control	Adequate	Management Override	Automate Inventory Control
B. Intangible Hazardous Materials	Improper Storage/Disposal	Remote	Significant	Public Works	Manual Inventory Control	Adequate	N/A	Automate Fuel Inventory Control
Other Assets:								
A. Personal Information	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

FAA, Inc. Fraud Risk Assessment Form

Municipality: Town of Nantucket

Department: Department of Public Works

Fiscal Year: 2013

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI-FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Corruption:								
Bribery:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Embezzlement:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Aiding and Abetting:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Conflicts Of Interest:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Other Risks:								
None	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Human Resources

FAA, Inc. Risk Assessment Questionnaire

GENERAL RISK ASSESSMENT Risk Assessment Questionnaire - Summary

AGENCY	Town of Nantucket Human Resources Department		
CYCLE	Initial Assessment	SYSTEM	Fraud Risk
PREPARED BY	FAA, Inc	DATE: 11/28/2012	

Given the results of the risk assessment guideline and other factors I have considered, in my opinion, the system being assessed has the following risk to the agency:

	HIGH RISK (41 – 70)	Internal control evaluation required
18 Points =	MEDIUM RISK (18 – 40)	Internal control evaluation recommended on a cyclical basis.
	LOW RISK (0 – 17)	Internal control evaluation not required.

Please read the explanation of each risk category and evaluation factor on the following pages. Then **assign a rating value in the box provided below**. The rating should be from 0 to 5, with 0 being the lowest or no risk and 5 being the highest or maximum risk.

ASSIGNED RISK CATEGORY	EVALUATION FACTOR	NO.	RATING
General	Outside Interest	1	1.00
	Regulatory/Contractual	2	2.00
	Employee Turnover	3	0.00
Other Reviews and Audits	Audit Coverage	4	1.00
	Results of Prior Reviews	5	0.00
Specific Financial Risk Areas	Account Balance Size	6	0.00
	General Fund State	7	5.00
	Federal Assistance Programs	8	0.00
	Cash	9	0.00
	Merchandise	10	0.00
	Fixed Assets	11	0.00
System	Automation	12	3.00
	Decentralization	13	1.00
	Sensitive Data	14	5.00
		TOTAL	18.00

**FAA, Inc. Control Environment
General Control Policies and Procedures Questionnaire**

Municipality: Nantucket

Department: Human Resources

Fiscal Year: 2013

A. Integrity and Ethical Values

Yes No N/A

1. Does the agency have a code of ethical conduct that has been made available to all employees?
2. Does the code of conduct address policy for potential conflicts of interest?
3. Is there a procedure in place for employees to report fraudulent or dishonest acts?
4. Does Management take appropriate disciplinary action when necessary to enforce the code of conduct?

B. Commitment to Competence

Yes No N/A

5. Does management understand the knowledge and skills required to accomplish tasks?
6. Does the entity provide for applicable training of its employees?
7. Do accounting personnel appear to have sufficient expertise in selecting and applying applicable accounting principles?
8. Do accounting supervisors appear to have sufficient expertise to review accounting transactions for accuracy and compliance with rules and regulations?
9. Are sufficient training opportunities to improve competency and update employees on new policies and procedures available?

C. Management's Philosophy and Operating Style

Yes No N/A

10. Are principal accounting records and accounting employees at all locations under the supervision of the principal accounting officer?
11. Are management and operating decisions determined at appropriate levels?
12. Are policies and procedures consistent with statutory authority?
13. Does management review audit recommendations and take appropriate corrective action?
14. Is the internal control structure supervised and reviewed by management to determine if it is operating as intended?

D. Organizational Structure

Yes No N/A

15. Is there an organization chart clearly defining the lines of management authority and responsibility?
16. Is the organization chart current and accurate?
17. Are policies and procedures for authorizations established at a reasonably high level?
18. Have specific line of authority and responsibility been established to ensure compliance with federal and state laws and regulations?
19. Are all the agency's operations centralized or decentralized?
20. If decentralized, is monitoring of the areas adequate?

E. Assignment of Authority and Responsibility

Yes No N/A

21. Has management provided resources to ensure compliance with grant requirements and federal and state laws?
22. Is management actively involved in supervision of the various functions?
23. Has fiscal authority been formally delegated to specific management personnel?
24. Are responsibilities divided so that no single employee controls all phases of a transaction?

F. Human Resource Policies and Practices

Yes No N/A

25. Are competent personnel recruited?
26. Are accurate, up-to-date-position descriptions available?
27. Are managers and employees held accountable for satisfactory completion of performance elements?
28. Do all supervisors and managers have at least a working knowledge of the State's personnel policies and procedures?
29. Does each supervisor and manager have a copy or access to a copy of the State's personnel policies and procedures?
30. Does management ensure compliance with the department's personnel policies and procedures manual concerning hiring, training, promoting, and compensating employees?
31. Has management established backup plans for sudden or significant changes in personnel?
32. Are supervisors readily available to help personnel with non-routine problems?
33. Are external audits performed on a periodic basis?
34. Are background checks performed on certain people who have access to personal information, positions of accounting and financial oversight, and positions of trust?

**FAA, Inc. Computer Security
Control Policies and Procedures Questionnaire**

Municipality: Nantucket

Department: Human Resources

Fiscal Year: 2013

A. Control Activities / Information and Communication:

Yes No N/A

- | | | | |
|-------------------------------------|-------------------------------------|--------------------------|--|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 1. Does management determine the type of access a new employee should be given and communicate it to the appropriate personnel? |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 2. Once roles have been established for a new employee by the appropriate personnel are roles given back to management to confirm that appropriate access was granted? |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 3. Does management approve all changes made to roles? |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 4. Are terminated employees removed from the roles on the last day of service? |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 5. Are responsibilities segregated to assure that no one individual has entry and approval roles? |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 6. Does every user have a unique user-id/password? |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | a. Are user passwords kept secret from other users? |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | b. Are user passwords changed periodically? |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | c. Are users aware of the confidential nature of their passwords? |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 7. Does management restrict users' access to the minimum level needed to perform their job? |

FAA, Inc. Fraud Risk Assessment Form

Fiscal Year: 2013

Department: Human Resources Department

Municipality: Town of Nantucket

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI-FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Financial Reporting:								
Revenue Recognition:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Expenditures:								
Departmental Budget	FY Payments Timing	Remote	Insignificant	Human Resources	A/P Processing	Adequate	N/A	N/A
Health Insurance Trust	FY Payments Timing	Remote	Material	Human Resources	A/P Processing	Adequate	N/A	N/A
Workers' Compensation	FY Payments Timing	Remote	Significant	Human Resources	A/P Processing	Adequate	N/A	N/A
Balance Sheet/Management Estimates:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disclosures:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Other Reporting:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

FAA, Inc. Fraud Risk Assessment Form

Municipality: Town of Nantucket

Department: Human Resources Department

Fiscal Year: 2013

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI-FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Misappropriation of Assets:								
Cash/Checks/Credit Cards:								
A. Point of Sales	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
B. Accounts Receivable	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
C. Disbursement/Vendor	False Payments	Remote	Material	Human Resources	Vendor Controls Multiple Reviews	Adequate	Management Override	Periodic Testing By Accounting
D. Payroll	Falsified Employee Attendance Reports	Remote	Insignificant	Human Resources	Multiple Reviews	Inadequate – See Narrative	Management Override	Periodic Testing By Accounting
E. Other	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Inventory:								
A. Tangible:								
Fuel	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Equipment	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Small Tools	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
B. Intangible:								
Personal Information	Improper Storage or Accidental Disclosure	Reasonably Possible	Significant	Human Resources	Internal Department Controls	Inadequate	Loss of Personal Data	Increase Security of Record Storage
Other Assets:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

FAA, Inc. Fraud Risk Assessment Form

Fiscal Year: 2013

Municipality: Town of Nantucket Department: Human Resources Department

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI-FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Corruption:								
Bribery:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Embezzlement:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Aiding and Abetting:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Conflicts Of Interest:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Other Risks:								
None	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Nantucket Memorial Airport

FAA, Inc. Risk Assessment Questionnaire

GENERAL RISK ASSESSMENT Risk Assessment Questionnaire - Summary

AGENCY	Town of Nantucket Memorial Airport		
CYCLE	Initial Assessment	SYSTEM	Fraud Risk
PREPARED BY	FAA, Inc	DATE: 09/11/2012	

Given the results of the risk assessment guideline and other factors I have considered, in my opinion, the system being assessed has the following risk to the agency:

58 Points =	HIGH RISK (41 – 70)	Internal control evaluation required
	MEDIUM RISK (18 – 40)	Internal control evaluation recommended on a cyclical basis.
	LOW RISK (0 – 17)	Internal control evaluation not required.

Please read the explanation of each risk category and evaluation factor on the following pages. Then **assign a rating value in the box provided below**. The rating should be from 0 to 5, with 0 being the lowest or no risk and 5 being the highest or maximum risk.

ASSIGNED RISK CATEGORY	EVALUATION FACTOR	NO.	RATING
General	Outside Interest	1	5.00
	Regulatory/Contractual	2	3.00
	Employee Turnover	3	5.00
Other Reviews and Audits	Audit Coverage	4	0.00
	Results of Prior Reviews	5	5.00
Specific Financial Risk Areas	Account Balance Size	6	4.00
	General Fund State	7	5.00
	Federal Assistance Programs	8	4.00
	Cash	9	5.00
	Merchandise	10	5.00
	Fixed Assets	11	5.00
System	Automation	12	3.00
	Decentralization	13	4.00
	Sensitive Data	14	5.00
		TOTAL	58.00

**FAA, Inc. Control Environment
Control Policies and Procedures Questionnaire**

Municipality: Nantucket

Department: Memorial Airport

Fiscal Year: 2013

A. Integrity and Ethical Values

Yes No N/A

1. Does the agency have a code of ethical conduct that has been made available to all employees?
2. Does the code of conduct address policy for potential conflicts of interest?
3. Is there a procedure in place for employees to report fraudulent or dishonest acts?
4. Does Management take appropriate disciplinary action when necessary to enforce the code of conduct?

B. Commitment to Competence

Yes No N/A

5. Does management understand the knowledge and skills required to accomplish tasks?
6. Does the entity provide for applicable training of its employees?
7. Do accounting personnel appear to have sufficient expertise in selecting and applying applicable accounting principles?
8. Do accounting supervisors appear to have sufficient expertise to review accounting transactions for accuracy and compliance with rules and regulations?
9. Are sufficient training opportunities to improve competency and update employees on new policies and procedures available?

C. Management's Philosophy and Operating Style

Yes No N/A

10. Are principal accounting records and accounting employees at all locations under the supervision of the principal accounting officer?
11. Are management and operating decisions determined at appropriate levels?
12. Are policies and procedures consistent with statutory authority?
13. Does management review audit recommendations and take appropriate corrective action?
14. Is the internal control structure supervised and reviewed by management to determine if it is operating as intended?

D. Organizational Structure

Yes No N/A

15. Is there an organization chart clearly defining the lines of management authority and responsibility?
16. Is the organization chart current and accurate?
17. Are policies and procedures for authorizations established at a reasonably high level?
18. Have specific line of authority and responsibility been established to ensure compliance with federal and state laws and regulations?
19. Are all the agency's operations centralized or decentralized?
20. If decentralized, is monitoring of the areas adequate?

E. Assignment of Authority and Responsibility

Yes No N/A

21. Has management provided resources to ensure compliance with grant requirements and federal and state laws?
22. Is management actively involved in supervision of the various functions?
23. Has fiscal authority been formally delegated to specific management personnel?
24. Are responsibilities divided so that no single employee controls all phases of a transaction?

F. Human Resource Policies and Practices

Yes No N/A

25. Are competent personnel recruited?
26. Are accurate, up-to-date-position descriptions available?
27. Are managers and employees held accountable for satisfactory completion of performance elements?
28. Do all supervisors and managers have at least a working knowledge of the State's personnel policies and procedures?
29. Does each supervisor and manager have a copy or access to a copy of the State's personnel policies and procedures?
30. Does management ensure compliance with the department's personnel policies and procedures manual concerning hiring, training, promoting, and compensating employees?
31. Has management established backup plans for sudden or significant changes in personnel?
32. Are supervisors readily available to help personnel with non-routine problems?
33. Are external audits performed on a periodic basis?
34. Are background checks performed on certain people who have access to personal information, positions of accounting and financial oversight, and positions of trust?

**FAA, Inc. Computer Security
Control Policies and Procedures Questionnaire**

Municipality: Nantucket

Department: Memorial Airport

Fiscal Year: 2013

A. Control Activities / Information and Communication:

Yes No N/A

- 1. Does management determine the type of access a new employee should be given and communicate it to the appropriate personnel?
- 2. Once roles have been established for a new employee by the appropriate personnel are roles given back to management to confirm that appropriate access was granted?
- 3. Does management approve all changes made to roles?
- 4. Are terminated employees removed from the roles on the last day of service?
- 5. Are responsibilities segregated to assure that no one individual has entry and approval roles?
- 6. Does every user have a unique user-id/password?
 - a. Are user passwords kept secret from other users?
 - b. Are user passwords changed periodically?
 - c. Are users aware of the confidential nature of their passwords?
- 7. Does management restrict users' access to the minimum level needed to perform their job?

FAA, Inc. Fraud Risk Assessment Form

Fiscal Year: 2013

Municipality: Town of Nantucket

Department: Municipal Airport

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI-FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Financial Reporting:								
Revenue Recognition:	Improper Classification/Timing	Probable	Material	Airport and Accounting	Reconciliation	Adequate	Management Override	Periodic Testing By Accounting
Expenditure Recognition:	Improper Classification/Timing	Probable	Material	Airport and Accounting	Reconciliation	Adequate	Management Override	Periodic Testing By Accounting
Balance Sheet/Management Estimates:	Misstated Inventory	Reasonably Possible	Significant	Airport and Accounting	Inventory Control System	Adequate	Inaccuracy	Periodic Testing By Accounting
	Misstated Compensated Absences	Remote	Insignificant	Airport and Accounting	Automated Attendance & Payroll System	Adequate	Management Override	Periodic Testing By Accounting
Disclosures:	Misstated Fund Balances/Reserves	Reasonably Possible	Material	Airport and Accounting	Reconciliation	Adequate	Management Override	Periodic Testing By Accounting
	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Other Reporting:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

FAA, Inc. Fraud Risk Assessment Form

Municipality: Town of Nantucket

Department: Municipal Airport

Fiscal Year: 2013

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI-FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Misappropriation of Assets:								
A. Point of Sales	Unrecorded Fuel/Services Sales	Remote	Significant	Airport FBO Staff	Segregation of Duties Automated System	Adequate	Management Override	Periodic Testing By Accounting
	Unrecorded Caterer Sales	Remote	Insignificant	Airport FBO Staff	Segregation of Duties Automated System	Adequate	Management Override	Periodic Testing By Accounting
	Unreported Attire Sales	Remote	Insignificant	Airport FBO Staff	Segregation of Duties Automated System	Adequate	Management Override	Periodic Testing By Accounting
	Unreported Taxi Cab Sticker Sales	Reasonably Possible	Insignificant	Airport Finance Staff	Stickers Color Coded By Year	Inadequate	Undocumented Sales	Implement Use of Pre-Numbered Stickers
B. Accounts Receivable	Parking Lot Tokens/Cash Theft	Reasonably Possible	Significant	Airport Finance Staff	Automated System Multiple Employee Transactions	Adequate	Management Override	Periodic Testing By Accounting
	Unreported Transient Tie Down Sales/Payments	Remote	Insignificant	Airport Finance Staff	Automated Billing System	Adequate	Management Override	Periodic Testing By Accounting
	Hanger Lease Transactions Fraud	Remote	Significant	Airport Finance Staff	Automated Billing/AR System	Adequate	Management Override	Periodic Testing By Accounting
	Tie Down Lease Transactions Fraud	Remote	Insignificant	Airport Finance Staff	Automated Billing/AR System	Adequate	Management Override	Periodic Testing By Accounting
	Terminal/Land Lease Transactions Fraud	Remote	Significant	Airport Finance Staff	Automated Billing/AR System	Adequate	Management Override	Periodic Testing By Accounting

FAA, Inc. Fraud Risk Assessment Form

Municipality: Town of Nantucket

Department: Municipal Airport

Fiscal Year: 2013

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI- FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Misappropriation of Assets: Continued								
C. Disbursement/Vendor	False Payments	Remote	Insignificant	Airport Finance Staff	Vendor Controls	Adequate	Management Override	Periodic Testing By Accounting
D. Payroll	Falsified Employee Attendance Reports	Remote	Insignificant	Airport Management	Multiple Reviews	Inadequate – See Narrative	Management Override	Periodic Testing By Accounting
E. Other	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Inventory:								
A. Tangible Fuel	Theft/Misuse	Remote	Significant	Airport FBO/Finance Staff	Manual Inventory Control	Adequate	Management Override	Automate Inventory Control
Equipment	Theft/Misuse	Remote	Significant	Airport Staff	Manual Inventory Control	Adequate	Management Override	Automate Inventory Control
Small Tools	Theft/Misuse	Remote	Insignificant	Airport Staff	Manual Inventory Control	Adequate	Management Override	Automate Inventory Control
B. Intangible Hazardous Materials	Improper Storage/Disposal	Remote	Significant	Airport Staff	Manual Inventory Control	Adequate	Management Override	Automate Inventory Control
Other Assets:								
Personal Information	Improper Storage/Disclosure	Remote	Significant	Airport Staff	Internal Departmental Controls	Adequate	Management Override	Periodic Testing By Accounting

FAA, Inc. Fraud Risk Assessment Form

Municipality: Town of Nantucket

Department: Municipal Airport

Fiscal Year: 2013

	1. IDENTIFIED FRAUD RISKS AND SCHEMES	2. LIKELIHOOD	3. SIGNIFICANCE	4. PEOPLE AND/OR DEPARTMENT	5. EXISTING ANTI-FRAUD CONTROLS	6. CONTROLS EFFECTIVENESS ASSESSMENT	7. RESIDUAL RISKS	8. FRAUD RISK RESPONSE
Corruption:								
Bribery:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Embezzlement:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Aiding and Abetting:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Conflicts Of Interest:	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Other Risks:								
None	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A