Central Florida Expressway Authority

2013 COSO Framework Governance Review

June 3, 2015

protiviti®
Risk & Business Consulting.
Internal Audit.

Table of Contents

This document has been prepared for use by CFX management, audit committee, and board of directors. This report provides information about the condition of risks and internal controls at one point in time. Future events and changes may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

Executive Summary

Overview

In accordance with the fiscal year 2015 Internal Audit Plan, Internal Audit performed a review of the governance structure at the Central Florida Expressway Authority (the Authority) using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2013 Internal Control – Integrated Framework as a guide to perform the review. The COSO 2013 Framework is one of the most widely used internal control frameworks in the world and contains leading practice guidance for establishing effective governance procedures and internal controls.

Originally formed in 1985, COSO is a joint initiative of five private sector organizations (the IIA, AICPA, IMA, FEI, and American Accounting Association) and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.

On May 14, 2013, COSO released an updated version of the Internal Control - Integrated Framework that was first published in 1992 to assess and report on the design and operating effectiveness of an organization's internal controls. The updated 2013 COSO Framework outlines 17 principles and provides 77 supporting points of focus within each of the five foundational components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities.

Objectives

The objective of the review was to provide recommendations to enhance the Authority’s overall governance through the identification of entity-level control design opportunities that might exist when comparing existing structure to the 2013 COSO Framework of leading practices.

Scope and Approach

Internal Audit performed the following activities to complete the 2013 COSO Framework Governance review:

1. Reviewed existing governance documentation and conducted interviews with key personnel to obtain an understanding of current state governance structure, policies, procedures, and internal controls.
2. Documented and compared the Authority’s governance processes to the 17 COSO principles and 77 points of focus.
3. Reviewed internal control documentation to evaluate the Control Design Effectiveness of governance controls in place at CFX.
4. Identified opportunities and developed recommendations for enhancing the CFX governance structure.

No internal control testing was performed as part of this review.

Summary of Results

Internal Audit reviewed and identified approximately 80 well-designed governance controls currently in place at the Authority covering the 17 principles within the COSO Framework. Overall, the Authority has many of the governance related controls typically seen within a publicly traded company environment. This is commendable as the Authority has not performed an assessment of this nature in previous years.

Based upon the results of the review, Internal Audit identified the following six opportunities for CFX to consider to enhance the governance structure:

Control Environment

- Consider realignment of the public records process
- Perform an annual training needs assessment and formalize the training request process
- Enhance the annual performance evaluation process to include employee self-assessment and goal-setting activities

Control Activities

- Update Human Resources and Informational Technology (IT) desktop procedures

Information and Communication

- Develop Board and Committee checklists to monitor compliance with responsibilities
- Post the internal ethics hotline information on the intranet

Summary of COSO Framework

COSO Components	Principles	# of Points of Focus
CONTROL ENVIRONMENT	Demonstrates commitment to integrity and ethical values	4
	Exercises oversight responsibility	4
	Establishes structure, authority and responsibility	3
	Demonstrates commitment to competence	4
	Enforces accountability	5
RISK ASSESSMENT	Specifies relevant objectives	5
	Identifies and analyzes risk	5
	Assesses fraud risk	4
	Identifies and analyzes significant change	3
CONTROL ACTIVITIES	Selects and develops control activities	6
	Selects and develops general controls over technology	4
	Deploys through policies and procedures	6
INFORMATION & COMMUNICATION	Uses relevant information	5
	Communicates internally	4
	Communicates externally	5
MONITORING ACTIVITIES	Conducts ongoing and/or separate evaluations	7
	Evaluates and communicates deficiencies	3

This document has been prepared for use by CFX management, audit committee, and board of directors. This report provides information about the condition of risks and internal controls at one point in time. Future events and changes may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

Detailed Observations

COSO Principle and POF	Observation	Recommendation	Significance	Management Response / Owner / Due Date
Control Environment				
Principle 2. Board Exercises Oversight Responsibility Over Internal Control POF 5: Establishes oversight responsibilities	Based on leading practice, public records management is generally performed by one of the following departments: 1. Communications Department 2. Legal Department 3. Centralized Records Office that stores all public documents 4. Department liaisons Currently, the Authority's public records function is managed by the Procurement Department, which utilizes department liaisons to aid in responding to complex public records requests.	The Authority should consider revising the management of public records to align with leading practice, if the realignment would improve the efficiency or effectiveness of the public records process. To align with leading practice, the Authority should consider designating responsibility for public records management to the Communications or Legal Department.	Low	The Authority has realigned the public records management function to report to the Communications Department. Laura Kelley, Executive Director Complete
Principle 4. Demonstrates Commitment to Competence POF 13: Evaluates competence and addresses shortcomings	The Authority's department managers identify staff training needs and approve the training. Although staff training budgets are included in the Human Resource (HR) budget, the Human Resource department does not monitor the training needs of the organization. Leading practice is for Human Resources to perform periodic assessments of the training needs across the organization to promote development, competency, and continuing education. Additionally, a formalized training request process is not in place to document the business reason for each training expenditure and to ensure the appropriate approvals are obtained.	To incorporate leading practice, the Authority should perform an annual training needs assessment during the performance evaluation process to identify development opportunities throughout the organization. The Authority should also develop an HR Training Request Form to document the business reason for each training, cost, attendees, and Human Resources approval. The addition of the form will formalize the oversight process for training requests and help ensure training expenditures align with business needs, goals, and budgetary restrictions.	Medium	Concur. Heidi Klingensmith, Human Resources Manager 12/31/2015

Detailed Observations

COSO Principle and POF	Observation	Recommendation	Significance	Management Response / Owner / Due Date
Control Environment				
Principle 5. Enforces Accountability POF 17: Establishes performance measures, incentives, and rewards	Annual employee performance evaluations are completed by each employee's supervisor and reviewed with the employee. Employees are allowed to provide documented responses and comments within the evaluation form. However, there is an opportunity to improve the effectiveness of the performance evaluation and employee accountability through annual employee goal-setting discussions.	A leading practice is to incorporate employee goal-setting into the annual performance evaluation process. The employee's progress against goals can then be tracked and evaluated annually to create accountability in the performance evaluation process. To accomplish this, the Authority should implement an employee self-review and questionnaire in the evaluation form to facilitate employee involvement in the evaluation process. The self-review and questionnaire should be focused on obtaining feedback from employees regarding their perception of performance, areas for improvement, career development goals, and training needs.	Medium	Concur. Heidi Klingensmith, Human Resources Manager 12/31/2015

Detailed Observations

COSO Principle and POF	Observation	Recommendation	Significance	Management Response / Owner / Due Date
Control Activities				
Principle 12. Deploys Controls through Policies and Procedures POF 48: Establishes policies and procedures to support deployment of management's directives	Written procedures are an integral component of the infrastructure surrounding each critical business process. Procedures help govern, in writing, the actions necessary to fulfill the organization's policy for operations The IT and HR departments have not updated desktop procedural documents with the appropriate level of detail to provide guidance in the pursuit of achieving the objectives of the process, help reduce misunderstanding, and increase distribution of pertinent information to those involved in the process.	The Authority should identify and update the desktop procedures for key processes within the IT and HR departments to include the appropriate level of detail. The Desktop Procedures should allow anyone generally competent for the position to perform the job duties.	Medium	Concur. Heidi Klingensmith, Human Resources Manager Joann Chizlett, Director of Information Technology 2/28/2016

Detailed Observations

COSO Principle and POF	Observation	Recommendation	Significance	Management Response / Owner / Due Date
Information and Communication				
Principle 14. Communicates Internally POF 60: Communicates with the board of directors	The Authority's Audit Committee Charter, detailing the responsibility of the committee, has been summarized and developed into a checklist to enable ease of monitoring the Audit Committee's compliance with the requirements of the charter. However, the Authority has not developed checklists to aid the Board, Finance Committee, Operations Committee, and Right of Way Committee in monitoring compliance with their respective responsibilities.	As a leading practice to help Board members and committee members ensure they fulfill their responsibilities on an annual basis, the Authority should establish checklists that summarize key requirements and responsibilities of the Board, Finance Committee, Operations Committee, and Right of Way Committee. The Authority's Recording Secretary for the Board and Committees should use the checklist to monitor compliance and notify the Board and the Committees of upcoming compliance activities.	High	Concur. Laura Kelley, Executive Director 9/30/2015
Principle 14. Communicates Internally POF 61: Provides separate communication lines	The Authority has a whistleblower hotline (the "Make A Difference" hotline) for employees to anonymously report allegations of fraudulent or unethical behavior to the independent administrator. The whistleblower hotline contact information is posted in the Authority's employee break room and Employee Handbook. Leading practice for ethics hotline communication is to also post the hotline information on the internal intranet.	To enhance communication and awareness, the Authority should consider posting the Make A Difference hotline contact information on the organization's internal intranet to reflect leading practice and to allow for convenient, easy access to the information.	Low	Concur. Laura Kelley, Executive Director 8/30/2015

Appendix

Appendix – 2013 COSO Framework

Control Environment			
Principles		Points of Focus	
1	Demonstrates a Commitment to Integrity and Ethical Values	1	Sets the tone at the top
		2	Establishes standards of conduct
		3	Evaluates adherence to standards of conduct
		4	Addresses deviations in a timely manner
2	Board Exercises Oversight Responsibility Over Internal Control	5	Establishes oversight responsibilities
		6	Applies relevant expertise
		7	Operates independently
		8	Provides oversight of the system of internal control including Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities
3	Management Establishes Structures, Authorities and Responsibilities	9	Considers all structures of the entity
		10	Establishes reporting lines
		11	Defines, assigns, and limits authorities and responsibilities
4	Demonstrates Commitment to Competence	12	Establishes policies and practices
		13	Evaluates competence and addresses shortcomings
		14	Attracts, develops, and retains individuals
		15	Plans and prepares for succession
5	Enforces Accountability	16	Enforces accountability through structures, authorities and responsibilities
		17	Establishes performance measures, incentives, and rewards
		18	Evaluates performance measures, incentives, and rewards for ongoing relevance
		19	Considers excessive pressures
		20	Evaluates performance and rewards or disciplines

Appendix – 2013 COSO Framework

Risk Assessment			
Principles		**Points of Focus**	
6	Specifies Suitable Objectives	21a	Reflects management’s choices
		22a	Considers tolerances for risk
		23	Includes operations and financial performance goals
		24	Forms a basis for committing of resources
		21b	Complies with applicable accounting standards
		22b	Considers materiality
		25	Reflects entity activities
		21c	Complies with externally established standards and frameworks
		22c	Considers the required level of precision
		25	Reflects entity activities
		21a	Reflects management’s choices
		22c	Considers the required level of precision
		25	Reflects entity activities
		21d	Reflects external laws and regulations
		22a	Considers tolerances for risk
7	Identifies and Analyzes Risks	26	Includes entity, subsidiary, division, operating unit, and functional levels
		27	Analyzes internal and external factors
		28	Involves appropriate levels of management
		29	Estimates significance of risks identified
		30	Determines how to respond to risks

Appendix – 2013 COSO Framework

Control Activities			
Principles		Points of Focus	
10	Selects and Develops Control Activities	38	Integrates with risk assessment
		39	Considers entity-specific factors
		40	Determines relevant business processes
		41	Evaluates a mix of control activity types
		42	Considers at what level activities are applied
		43	Addresses segregation of duties
11	Selects and Develops General Controls over Technology	44	Determines dependency between the use of technology in business processes and technology general controls
		45	Establishes relevant technology infrastructure control activities
		46	Establishes relevant security management process control activities
		47	Establishes relevant technology acquisition, development, and maintenance process control activities
12	Deploys Controls through Policies and Procedures	48	Establishes policies and procedures to support deployment of management's directives
		49	Establishes responsibility and accountability for executing policies and procedures
		50	Performs in a timely manner
		51	Takes corrective action
		52	Performs using competent personnel
		53	Reassesses policies and procedures

Appendix – 2013 COSO Framework

Information and Communication			
Principles		**Points of Focus**	
13	Uses Relevant Information	54	Identifies information requirements
		55	Captures internal and external sources of data
		56	Processes relevant data into information
		57	Maintains quality throughout processing
		58	Considers costs and benefits
14	Communicates Internally	59	Communicates internal control information
		60	Communicates with the board of directors
		61	Provides separate communication lines
		62	Selects relevant method of communication
15	Communicates Externally	63	Communicates to external parties
		64	Enables inbound communications
		65	Communicates with the board of directors
		66	Provides separate communication lines
		67	Selects relevant method of communication

This document has been prepared for use by CFX management, audit committee, and board of directors. This report provides information about the condition of risks and internal controls at one point in time. Future events and changes may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

Appendix – 2013 COSO Framework

Monitoring Activities			
Principles		Points of Focus	
16	Conducts Ongoing and/or Separate Evaluations	68	Considers a mix of ongoing and separate evaluations
		69	Considers rate of change
		70	Establishes baseline understanding
		71	Uses knowledgeable personnel
		72	Integrates with business processes
		73	Adjusts scope and frequency
		74	Objectively evaluates
17	Evaluates and Communicates Deficiencies	75	Assesses results
		76	Communicates deficiencies
		77	Monitors corrective actions

Powerful Insights.
Proven Delivery.®