protiviti®
Face the Future with Confidence

COSO ERM GOVERNANCE REVIEW

May 2020

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

Internal Audit, Risk, Business & Technology Consulting

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Overview

Overview

In accordance with the fiscal year 2020 Internal Audit Plan, Internal Audit reviewed the Central Florida Expressway Authority's (CFX) governance procedures and internal controls leveraging two frameworks, the COSO 2013 Internal Control Framework and the COSO 2017 ERM Framework, as leading practice guidelines.

Internal Audit last performed a review of the governance structure and related internal controls at CFX during fiscal year 2015. The review was performed using only the COSO 2013 Internal Control Framework as leading practice guidelines. 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. The 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.

In September 2017, COSO released an updated version of the Enterprise Risk Management - Integrated Framework that was first published in 2004 to enhance an organization's ability to manage uncertainty and to consider how much risk to accept as it strives to increase value. The updated COSO ERM Framework recognizes the importance of strategy and entity performance, further delineates enterprise risk management from internal control, and provides definitions and principles for all levels of management involved in designing, implementing, and conducting enterprise risk management practices. The principles are organized within each of the five interrelated Framework components: Governance and Culture, Strategy and Objective-Setting, Performance, Review and Revision, and Information, Communication, and Reporting.

Objectives

The objectives of this audit were to leverage the COSO 2013 Internal Control Framework and the COSO ERM Framework as benchmarks to evaluate the current state governance structure at CFX and provide recommendations to enhance CFX's overall governance structure.

EXECUTIVE SUMMARY

Project Scope and Approach

This review was performed using a four-phased approach as outlined below:

Phase I – Documentation of Current State Processes

Internal Audit worked with management through interviews and review of existing policies and procedures in order to refresh documentation of CFX's governance processes and internal controls relevant to the 17 Principles and 77 Points of Focus of the COSO 2013 Internal Control Framework. Details regarding the COSO 2013 Internal Control Framework are included in Appendix A.

Phase II –Review of Key Controls for Design Effectiveness

Internal Audit identified key controls relevant to the COSO 2013 Internal Control Framework and performed an evaluation of design effectiveness. A summary of the procedures performed, results, and observations are provided on the following pages.

Phase III – Enterprise Risk Management Exploration Sessions

Internal Audit interviewed executive management and reviewed CFX's processes, policies, and procedures related to risk management. Internal Audit further evaluated existing risk management practices against the COSO 2017 ERM Framework to identify opportunities for enhanced risk management in the following core areas: Risk Management Policies, Risk Measurement, Roles and Responsibilities, Data, and Monitoring.

Phase IV – Benchmark Against Frameworks and Develop Recommendations

Using the knowledge gathered in the previous phases and the principles contained in the COSO 2013 Internal Control Framework and COSO 2017 ERM Framework as leading practice guidance, Internal Audit developed recommendations and opportunities for CFX to consider to enhance its overall governance infrastructure and risk management procedures.

EXECUTIVE SUMMARY

Summary of Procedures and Results – COSO 2013 Internal Control Review

Internal Audit reviewed and identified 94 governance controls currently in place at CFX covering the 17 principles and 77 points of focus within the COSO 2013 Internal Control Framework. During the time of last audit in 2015, six opportunities for improvement were identified, and all six opportunities were addressed by CFX as confirmed by Internal Audit as part of this review.

For the current review, the table below provides an overview of the areas reviewed under the COSO 2013 Internal Control Framework. No gaps in internal control design were identified within CFX's existing governance processes; however, one opportunity for potential improvement was identified. Further details are provided in the Detailed Observations section of this report. The COSO 2013 Framework 17 principles and 77 points of focus are outlined in Appendix A.

Foundational Component	Principles	Total Controls Reviewed	Number of Observations	Relative Priority
Control Environment	▪ Demonstrates a Commitment to Integrity and Ethical Values ▪ Board Exercises Oversight Responsibility Over Internal Control ▪ Management Establishes Structures, Authorities and Responsibilities ▪ Demonstrates Commitment to Competence ▪ Enforces Accountability	21	0	N/A
Risk Assessment	▪ Specifies Suitable Objectives ▪ Identifies and Analyzes Risks ▪ Assesses Fraud Risk ▪ Identifies and Analyzes Significant Change	25	0	N/A
Control Activities	▪ Selects and Develops Control Activities ▪ Selects and Develops General Controls over Technology ▪ Deploys Controls through Policies and Procedures	16	1	**Moderate**
Information & Communication	▪ Uses Relevant Information ▪ Communicates Internally ▪ Communicates Externally	22	0	N/A
Monitoring Activities	▪ Conducts Ongoing and/or Separate Evaluations ▪ Evaluates and Communicates Deficiencies	10	0	N/A
	TOTALS:	**94**	**1**	

protiviti

EXECUTIVE SUMMARY

Summary of Procedures and Results – COSO 2017 Enterprise Risk Management Review

In addition to leveraging the COSO 2013 Internal Control Framework for this review, Internal Audit also considered leading practices for risk management as outlined in the COSO 2017 ERM Framework. An evaluation of enterprise risk management practices had not previously been performed for CFX.

The table below provides an overview of the areas reviewed leveraging the COSO 2017 ERM Framework as a guide. Internal Audit identified four opportunities for potential enhancement to current risk management practices under the framework. Further details are provided in the Enhancement Opportunities section of this report. The COSO 2017 ERM Framework components and principles are outlined in Appendix B.

Foundational Component	Principles	Enhancement Opportunities
Risk Governance and Culture	▪ Exercise Board Risk Oversight ▪ Establishes Governance and Operating Model ▪ Defines Desired Organizational Behaviors ▪ Demonstrates Commitment to Integrity and Ethics ▪ Enforces Accountability ▪ Attracts, Develops, and Retains Talented Individuals	1
Risk, Strategy, and Objective-Setting	▪ Considers Risk and Business Context ▪ Defines Risk Appetite ▪ Evaluates Alternative Strategies ▪ Considers Risk while Establishing Business Objectives ▪ Defines Acceptable Variation in Performance	1
Risk in Execution	▪ Identifies Risk in Execution ▪ Assesses Severity of Risk ▪ Prioritizes Risks ▪ Identifies and Selects Risk Responses ▪ Assesses Risk in Execution ▪ Develops Portfolio View	1
Risk Information, Communication, and Reporting	▪ Uses Relevant Information ▪ Leverages Information Systems ▪ Communications Risk Information ▪ Reports on Risk, Culture, and Performance	1
Monitoring Enterprise Risk Management Performance	▪ Monitors Substantial Change ▪ Monitors Enterprise Risk Management	0
	TOTAL:	**4**

DETAILED OBSERVATIONS

DETAILED OBSERVATIONS

Observation 1 – Business Continuity Documentation

Relative Priority

Moderate

Control Environment

Risk Assessment

Control Activities

Information & Communication

Monitoring Activities

Observation

Business Continuity plans define processes and procedures for restoring a business or department to normal operating capacity following disruptive events of various kinds. Although CFX currently has Business Continuity plans in place for several departments, no plans are currently documented for the Infrastructure department and its components: Construction, Engineering, Maintenance, and Traffic Operations. Without a departmental-specific Business Continuity plan, the resumption of critical business processes could be delayed for an extended amount of time until backup, manual, or alternate arrangements are made.

Recommendation

Management should create a formalized business continuity plan for the Infrastructure department, including reference to each component. Plans should include items such as recovery teams and responsibilities, manual workaround procedures, and alternate work locations. In conjunction with Executive Management and the Information Technology department, the Infrastructure department should determine how additional resources (laptops, desktops, workstations, etc.) would be procured, if necessary, and the length of time it would take to obtain and properly configure these resources to the point where they could be utilized to establish connections with key systems in the event a recovery is needed.

Management Response

Management concurs.

Management Action Plan

CFX will develop business continuity documentation for each component of the Infrastructure department (and validate that third parties have one in place) that outlines the expectations for resuming business operations after a crisis.

Action Plan Owner / Due Date

Glenn Pressimone, Chief of Infrastructure; 12/31/2020

ENHANCEMENT OPPORTUNITIES

ENHANCEMENT OPPORTUNITIES

Opportunity 1 – Define and Assign Responsibility for Risk Management

Foundational Component	Relevant Principles	Fundamental Concepts
Risk Governance and Culture	#2) Establishes Governance and Operating Model	Enterprise Risk Management Structures

Enhancement Opportunity

Leading practice includes establishing reporting lines and structures within the organization to understand strategic risk, define responsibilities for risk management, and evaluate execution of strategy and business objectives from a risk management perspective.

CFX should consider establishing a formal, internal, management-led Risk Management Working Group to define and discuss key risks in the context of overall business strategy, delegate responsibilities for enterprise risk management, and support monitoring enhancements for key strategic risks. A formal Working Group could improve ownership over risk identification and support delegation of responsibility and accountability for risk mitigation.

Management Action Plan

CFX will organize a Risk Management Working Group with the following features:

- Responsible Party/Organizer – Risk Manager
- Members - Chief Finance Officer, Chief of Technology/Operations, Risk Manager, others may be added as needed
- Frequency – At the discretion of the Group, or at least semi-annually
- Agenda – Agenda topics should be determined by the responsible party and may include risks from the Strategic Plan or Risk Model, prior audit recommendations, risk monitoring needs, and other topics.

Action Plan Owner / Due Date

Lisa Lumbard, Chief Financial Officer; 12/31/2020

ENHANCEMENT OPPORTUNITIES

Opportunity 2 – Integrate Risk with Strategy Setting

Foundational Component	Relevant Principles	Fundamental Concepts
Risk, Strategy, and Objective-Setting	#10) Considers Risk while Establishing Business Objectives	Understanding the Implications of Chosen Business Objectives

Enhancement Opportunity

Based on leading practice, risk should be integrated into strategic planning such that adequate consideration of the risk implications of strategic decisions is made during the organization's strategy setting process.

Currently, CFX considers risk implicitly in the development of the 3-Year Strategic Plan, which graphically represents key business goals, strategies, tactics, and performance measures.

To better integrate consideration of risk into strategy setting, CFX should consider adding a "risk layer" to its 3-Year Strategic Plan in order to consider risks inherent in each key business goal and strategy.

Management Action Plan

The Risk Management Working Group will include an agenda item to solicit feedback from each relevant department regarding key strategic risks. The Risk Management Working Group, in coordination with management, will update the Three-Year Strategic Plan with the strategic risks for each strategic goal.

Action Plan Owner / Due Date

Lisa Lumbard, Chief Financial Officer; 3/31/2021

ENHANCEMENT OPPORTUNITIES

Opportunity 3 – Align Risk Response with Risk Appetite

Foundational Component	Relevant Principles	Fundamental Concepts
Risk in Execution	#15) Identifies and Selects Risk Responses	Considering Costs and Benefits of Risk Responses

Enhancement Opportunity

Effective risk management practices consider the potential costs and benefits of a risk response as well as the impact of a risk response on the entity's performance towards business objectives. A misalignment of risk response and risk appetite with the entity's performance goals can lead to excessive risk-taking or hinder performance.

CFX requires vendors to maintain levels of insurance coverage as specified in each contract. Those requirements, which extend to the size, type and rating of the insurance underwriter, are largely determined by the insurance broker, and are relatively standard across vendor contracts regardless of the size and relative risk of the contract.

As CFX fills the newly created Risk Manager position, CFX should consider applying risk-based vendor management concepts when assessing the cost and benefit of contractual requirements for vendor insurance coverages and defining coverage requirements.

Management Action Plan

The Risk Management Working Group will include an agenda item to solicit feedback from each relevant department, and, in coordination with the Procurement Department, will propose updates to current vendor insurance requirements to incorporate risk-based vendor management concepts.

Action Plan Owner / Due Date

Lisa Lumbard, Chief Financial Officer; 3/31/2021

ENHANCEMENT OPPORTUNITIES

Opportunity 4 – Utilize Data to Monitor Risk

Foundational Component	Relevant Principles	Fundamental Concepts
Risk Information, Communication and Reporting	#18) Uses Relevant Information	Determining Data Requirements

Enhancement Opportunity

Effective risk monitoring requires data on key risks that is relevant, accessible, accurate, timely, reliable, and complete.

While the data available to CFX employees covers a variety of functional areas and strategic risks, data availability and data quality could be improved in the following areas to support effective monitoring of strategic risks:

- Roadway maintenance performance
- Back-office customer satisfaction
- Certain back-office transaction reports
- Utilization of Minority / Women / Disadvantaged Business Enterprises

CFX should consider opportunities to utilize technology to improve available data in these areas and to facilitate monitoring capabilities where possible. Where RFP or software implementation is already in progress, CFX should consider risk monitoring data needs during the procurement or implementation requirements for those new systems.

CFX should also consider developing a new standard IT template and procedures for capturing resource cost and expected benefit for new data and reporting requests in order to better support prioritization of IT resources.

Management Action Plan

The Risk Management Working Group will include an agenda item to monitor status of each of the above data requests and follow up as needed. Additionally, the Risk Management Working Group will coordinate with the Technology / Operations Department to refine the ticketing system by which reporting requests are made and will support development of that system towards capture of relevant cost / benefit information.

Action Plan Owner / Due Date

Lisa Lumbard, Chief Financial Officer; 6/30/2021

APPENDIX A

COSO 2013 Internal Control Framework

APPENDIX A

COSO 2013 Internal Control Framework

COSO Components	Principles	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

APPENDIX A

COSO 2013 Internal Control 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 A

COSO 2013 Internal Control 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

APPENDIX A

COSO 2013 Internal Control Framework

Risk Assessment (Continued)			
Principles		**Points of Focus**	
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
8	Assesses Fraud Risk	31	Considers various types of fraud
		32	Assesses incentives and pressures
		33	Assesses opportunities
		34	Assesses attitudes and rationalizations
9	Identifies and Analyzes Significant Change	35	Assesses changes in the external environment
		36	Assesses changes in the business model
		37	Assesses changes in leadership

APPENDIX A

COSO 2013 Internal Control 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 A

COSO 2013 Internal Control 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

APPENDIX A

COSO 2013 Internal Control 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

APPENDIX B

COSO 2017 Enterprise Risk Management Framework

APPENDIX B

COSO 2017 Enterprise Risk Management Framework

Enterprise Risk Management			
Components	**Components and Descriptions**	**Principles**	
1	**Risk Governance and Culture** - Risk governance and culture together form a basis for all other components of enterprise risk management.	1	Exercise Board Risk Oversight
		2	Establishes Governance and Operating Model
		3	Defines Desired Organizational Behaviors
		4	Demonstrates Commitment to Integrity and Ethics
		5	Enforces Accountability
		6	Attracts, Develops, and Retains Talented Individuals
2	**Risk, Strategy, and Objective-Setting** - Enterprise risk management is integrated into the entity's strategic plan through the process of setting strategy and business objectives.	7	Considers Risk and Business Context
		8	Defines Risk Appetite
		9	Evaluates Alternative Strategies
		10	Considers Risk while Establishing Business Objectives
		11	Defines Acceptable Variation in Performance

APPENDIX B

COSO 2017 Enterprise Risk Management Framework

Enterprise Risk Management			
Components	**Components and Descriptions**	**Principles**	
3	**Risk in Execution** - An organization identifies and assesses risks that may impact the achievement of the entity's strategy and business objectives.	12	Identifies Risk in Execution
		13	Assesses Severity of Risk
		14	Prioritizes Risks
		15	Identifies and Selects Risk Responses
		16	Assesses Risk in Execution
		17	Develops Portfolio View
4	**Risk Information, Communication, and Reporting** - Communication is the continual, iterative process of providing, sharing, and obtaining information, which flows throughout the entity.	18	Uses Relevant Information
		19	Leverages Information Systems
		20	Communications Risk Information
		21	Reports on Risk, Culture, and Performance
5	**Monitoring Enterprise Risk Management Performance** - Monitoring enterprise risk management performance considers how well the enterprise risk management components are functioning over time and in light of substantial changes.	22	Monitors Substantial Change
		23	Monitors Enterprise Risk Management

Face the Future with Confidence

protiviti®