

# CENTRAL FLORIDA EXPRESSWAY AUTHORITY

**AGENDA**  
**CENTRAL FLORIDA EXPRESSWAY AUTHORITY**  
**AUDIT COMMITTEE MEETING**  
**June 17, 2020**  
**1:30 PM**

**Meeting location: Microsoft Teams Virtual Meeting**  
**Call (321) 430-0870**  
**Input Conference ID: 804 465 49#**

**A. CALL TO ORDER**

- B. PUBLIC COMMENT** – Pursuant to Executive Order 2020-69, issued by Governor Ron DeSantis, “local government bodies may utilize communications media technology, such as telephonic and video conferencing, as provided in section 120.54(5)(b)2., Florida Statutes,” in order to establish quorums. As such, procedures for all CFX public meetings have been temporarily modified to allow public meetings to occur remotely and reduce the spread of transmission of the COVID-19 virus. Any public comments to the Audit Committee were noticed and requested to be emailed to [AuditComments@cfxway.com](mailto:AuditComments@cfxway.com) and were to be received by 4 p.m. on June 16, 2020 to be included as part of the record.

Such comments were to be limited to any such items that are either identified on this meeting agenda as requiring action or anticipated to come before the Committee for action in reasonable future. Public comments will be read into the record except that if the comments exceeded 3 minutes in length, when read, they will only be attached as part of the minutes. In any case, all comments received were to be distributed electronically to all members in advance of the meeting date.

**C. APPROVAL OF THE MARCH 3, 2020 MINUTES** – (Action Item)

**D. INTERNAL AUDIT MATTERS** - Protiviti

1. Status Update: Fiscal 2020 Internal Audit Plan – (Info Item)
2. Review and Acceptance of Fiscal 2020 Internal Audit Reports – (Action Items)
  - a. COSO ERM Governance Review
  - b. RPA and Automation Review
  - c. P-Card and Gas Card Audit
  - d. Retail Transponder Sales Review
  - e. Marketing and Social Media Audit
  - f. 2021 Internal Audit Plan and Risk Assessment
3. Other Internal Audits – (Info Item)
  - a. Lane Scheduling and Customer Service Review – Cancelled
  - b. NIST Cyber Security Review - Update
  - c. Public Records and Information Management Review – Update
4. Annual Confirmation of No Disagreements with Management

**E. ANNUAL MANAGEMENT REVIEW OF INTERNAL CONTROL MATTERS – (Info Items)**

1. Effectiveness of the Internal Control System, Including IT Security and Control – Lisa Lumbard
2. Process for Assessing, Monitoring and Controlling Significant Risks – Lisa Lumbard
3. System for Monitoring Compliance with Laws and Regulations and Results of Investigation of any Instances of Non-Compliance – Woody Rodriguez
4. Adequacy, Administration and Compliance with the Authority's Code of Ethics – Woody Rodriguez
5. Procedures for "Hotline" Reporting – Woody Rodriguez

**F. ANNUAL DISCUSSION REGARDING INTERNAL AUDITOR PERFORMANCE AND EFFECTIVENESS – Kristy Mullane**

**G. ANNUAL DISCUSSION REGARDING AUDIT COMMITTEE AND INDIVIDUAL MEMBER PERFORMANCE – Kristy Mullane**

**H. CONFIRMATION OF COMPLETION OF RESPONSIBILITIES IN THE AUDIT COMMITTEE CHARTER – Protiviti**

**I. OTHER BUSINESS**

**J. ADJOURNMENT**

**THIS MEETING IS OPEN TO THE PUBLIC**

Section 286.0105, Florida Statutes, states that if a person decides to appeal any decision made by a board, agency, or commission with respect to any matter considered at a meeting or hearing, he or she will need a record of the proceedings, and that, for such purpose, he or she may need to ensure that a verbatim record of the proceedings is made, which record includes the testimony and evidence upon which the appeal is to be based.

In accordance with the Americans with Disabilities Act (ADA), if any person with a disability as defined by the ADA needs special accommodation to participate in this proceeding, then not later than two (2) business days prior to the proceeding, he or she should contact the Central Florida Expressway Authority at (407) 690-5000.

Persons who require translation services, which are provided at no cost, should contact CFX at (407) 690-5000 x5316 or by email at [franetta.dennis@CFXway.com](mailto:franetta.dennis@CFXway.com) at least three business days prior to the event.

**C.**

**Approval of  
Minutes**

# CENTRAL FLORIDA EXPRESSWAY AUTHORITY

**DRAFT MINUTES**  
**CENTRAL FLORIDA EXPRESSWAY AUTHORITY**  
**AUDIT COMMITTEE MEETING**  
**March 3, 2020**

**Location: Central Florida Expressway Authority**  
**4974 ORL Tower Road**  
**Orlando, FL 32807**  
**Pelican Conference Room 107**

---

Committee Members Present:

Kristy Mullane, Lake County Representative, Chairwoman  
Lorie Bailey Brown, Seminole County Representative  
Kaye Dover, Osceola County Representative  
Michelle McCrimmon, City of Orlando Representative  
Randy Singh, Orange County Representative

Committee Members Not Present:

Kathy Wall, Brevard County Representative

Also Present:

Lisa Lumbard, Chief Financial Officer  
Rita Moore, Recording Secretary/Executive Assistant  
Jeff Tecau, Protiviti  
Emily Picard, Protiviti  
Chris Porter, Protiviti  
David Taylor, Protiviti

**A. CALL TO ORDER**

The meeting was called to order at approximately 10:03 a.m. by Chairman Mullane.

Michelle McCrimmon, City of Orlando Representative, was welcomed to the Audit Committee.

All others in attendance introduced themselves.

Lisa Lumbard, Chief Financial Officer, announced the legal opinion of General Counsel, Woody Rodriguez, who was not present. It is the opinion of General Counsel that we no longer record the Audit Committee meetings since some of the information discussed in the meetings is not open to the Public.

**B. PUBLIC COMMENT**

There was no public comment.

**C. APPROVAL OF THE OCTOBER 30, 2019 MINUTES**

**A motion was made by Ms. Dover and seconded by Mr. Singh to approve the October 30, 2019 minutes as presented. The motion carried unanimously with five (5) members present voting AYE by voice vote; Ms. Wall was not present.**

**D. INTERNAL AUDIT MATTERS**

1. Status Update: Fiscal Year 2020 Internal Audit Plan

Jeff Tecau of Protiviti provided a brief introduction of Protiviti and their role at CFX for the new member, Ms. McCrimmon, City of Orlando Representative.

Jeff Tecau of Protiviti summarized the progress of the Fiscal Year 2020 Internal Audit Plan. Mr. Tecau informed the Committee that Fiscal Year 2020 Internal Audit is on schedule. Six (6) Audits have been completed to date; Prior Audit Recommendations, Procurement & Contract Billing Audits, DHSMV Data Security Assessment, DAVID Data Security Assessment, PCI Assessment with Report on Compliance, and Secure Code Review. Seven (7) Audits remain in process.

(This item was presented for information only. No formal committee action was taken.)

2. Review and Acceptance of Fiscal 2020 Internal Audit Reports – (Action Items)

a. Prior Audit Recommendations: Semi-Annual Follow Up

Emily Porter of Protiviti presented the Prior Audit Recommendations: Semi-Annual Follow Up report. She provided an update on certain items that were showing past due during the last report. Discussion was had between Protiviti and CFX around items showing past due because they are contingent upon new technology rollouts. It was decided to alter the completion dates and track based on the new completion dates. Five (5) of the Seven (7) in progress Audits were affected by the pending technology rollout.

Chairman Mullane posed the question about the timing of the technology rollout (system replacement). Discussion was had around a short hiatus due to testing issues.

**A motion was made by Ms. Dover and seconded by Mr. Singh to accept the Prior Audit Recommendations: Semi-Annual Follow Up report as presented. The motion carried unanimously with five (5) members present voting AYE by voice vote. Ms. Wall was not present.**

b. Procurement and Contract Billing Audit

Emily Picard of Protiviti presented the Procurement and Contract Billing Audit report with three findings (two findings were moderate and one low risk) Two contracts were selected to audit; Egis and Transcore.

Findings one (1) and findings two (2) were related to invoice processing on the Egis contract, it was recommended to implement a contract checklist to be utilized as a documentation tool moving forward.

Finding three (3) was related to ambiguous contract terms and vendor disputes on the Egis contract, it was recommended management establish an internal procedure for documenting vendor disputes and assigning decision making authority to appropriate representatives with the department and executive team for resolution of disputes.

A discussion was had around:

- The call center and image review contract. Ms. Lumbard stated that we are advertising for a new contractor on Sunday March 8<sup>th</sup>, 2020.
- Staff workload capacity in relation to implementing a checklist.
- Protiviti's involvement in reviewing the contract/agreement before it goes out? Mr. Tecau of Protiviti stated that they haven't historically, but as they put together the audit plan for the next year, we will look at the contract process.

**A motion was made by Ms. Dover and seconded by Ms. McCrimmon to accept the Procurement and Contract Billing Audit report as presented. The motion carried unanimously with five (5) members present voting AYE by voice vote. Ms. Wall was not present**

c. DHSMV Data Security Assessment

David Taylor of Protiviti presented the DHSMV Data Security Assessment report summarizing that the goal of this assessment is to ensure that information is protected, anyone who has access to it is supposed to have access. Mr. Taylor of Protiviti indicated the assessment was clean with no observations/findings.

A discussion was had about how it is monitored that the people who have access are using the system appropriately. Mr. Greer, Chief Technology Officer, stated that they log all activity over time and sample them from time to time. The State of Florida will ask questions about what was accessed if they have questions.

A discussion was had about the short time period of the assessment. David Taylor of Protiviti stated that this assessment is a "point in time" assessment.

**A motion was made by Ms. Dover and seconded by Ms. McCrimmon to accept the DHSMV Data Security Assessment report as presented. The motion carried unanimously with five (5) members present voting AYE by voice vote. Ms. Wall was not present.**

d. DAVID Data Security Assessment

David Taylor of Protiviti presented the DAVID Data Security Assessment report summarizing that this assessment is used to maintain driver's license numbers, social security numbers, and driver's license pictures. All lookups are logged and a memorandum of understanding (MOU) is in place. David Taylor of Protiviti indicated the assessment was clean with no observations/findings.

**A motion was made by Ms. McCrimmon and seconded by Ms. Dover to accept the DAVID Data Security Assessment report as presented. The motion carried unanimously with five (5) members present voting AYE by voice vote. Ms. Wall was not present.**

e. Payment Card Industry (PCI) Assessment with Report on Compliance

David Taylor of Protiviti presented the Payment Card Industry (PCI) Assessment with Report on Compliance summarizing that this assessment is used to ensure compliance with PCI. Noncompliance will result in the loss of ability to accept credit cards. Three (3) observations were noted. The system was not deleting calls in the sixty (60) day timeframe. This issue was resolved in eight (8) days. The second observation was related to strengthening network firewalls, new rules were put in place to strengthen it. This fix took two (2) days. The third observation was related to Active directory updates. This fix took one (1) day to complete.

**A motion was made by Mr. Singh and seconded by Ms. Dover to accept the Payment Card Industry (PCI) Assessment with Report on Compliance as presented. The motion carried unanimously with five (5) members present voting AYE by voice vote; Ms. Wall was not present.**

f. Secure Code Review

David Taylor of Protiviti presented the Secure Code Review report summarizing that this assessment is used to test how web applications and mobile applications are developed and level of security. Two observations were noted. Failure to sanitize in the web app was considered a medium risk observation. The second observation noted information not being validated.

Discussion was had around the timing of these tests and the instructions the Protiviti team is given regarding how hard they test for security.

**E. ANNUAL REVIEW AND APPROVAL OF AUDIT COMMITTEE CHARTER**

Ms. Lumbard summarized the changes made to the Audit Committee Charter. The language was changed around the Chairman of the Audit Committee being required at all Board Meetings. Additionally, Committee Members can now vote by phone as long as there is a physical quorum in the room.

Discussion was had around adding the succession language. Ms. Lumbard confirmed that it was added.

**A motion was made by Ms. Dover and seconded by Ms. Bailey Brown to accept the Audit Committee Charter as presented. The motion carried unanimously with five (5) members present voting AYE by voice vote. Ms. Wall was not present.**

**F. INTERNAL AUDIT BUDGET FOR FISCAL YEAR 2021**

Ms. Lumbard presented the internal audit budget for fiscal year 2021.

Discussion was had around whether Protiviti would come in on budget. Mr. Tecau stated that Protiviti is tracking just under budget.

**A motion was made by Mr. Singh and seconded by Ms. Dover to accept the internal audit budget for Fiscal Year 2021 as presented. The motion carried unanimously with five (5) members present voting AYE by voice vote. Ms. Wall was not present.**



**G. OTHER BUSINESS**

Discussion was had regarding the means that E-PASS customers use to hide their license plates to avoid tolls. Ms. Lumbard stated that the Florida Highway Patrol assigned to CFX roads monitors for any activity that obscures or hides a license plate.

**H. ADJOURNMENT**

Chairman Mullane adjourned the meeting at approximately 11:43 a.m.

Minutes approved on \_\_\_\_\_, 2020.

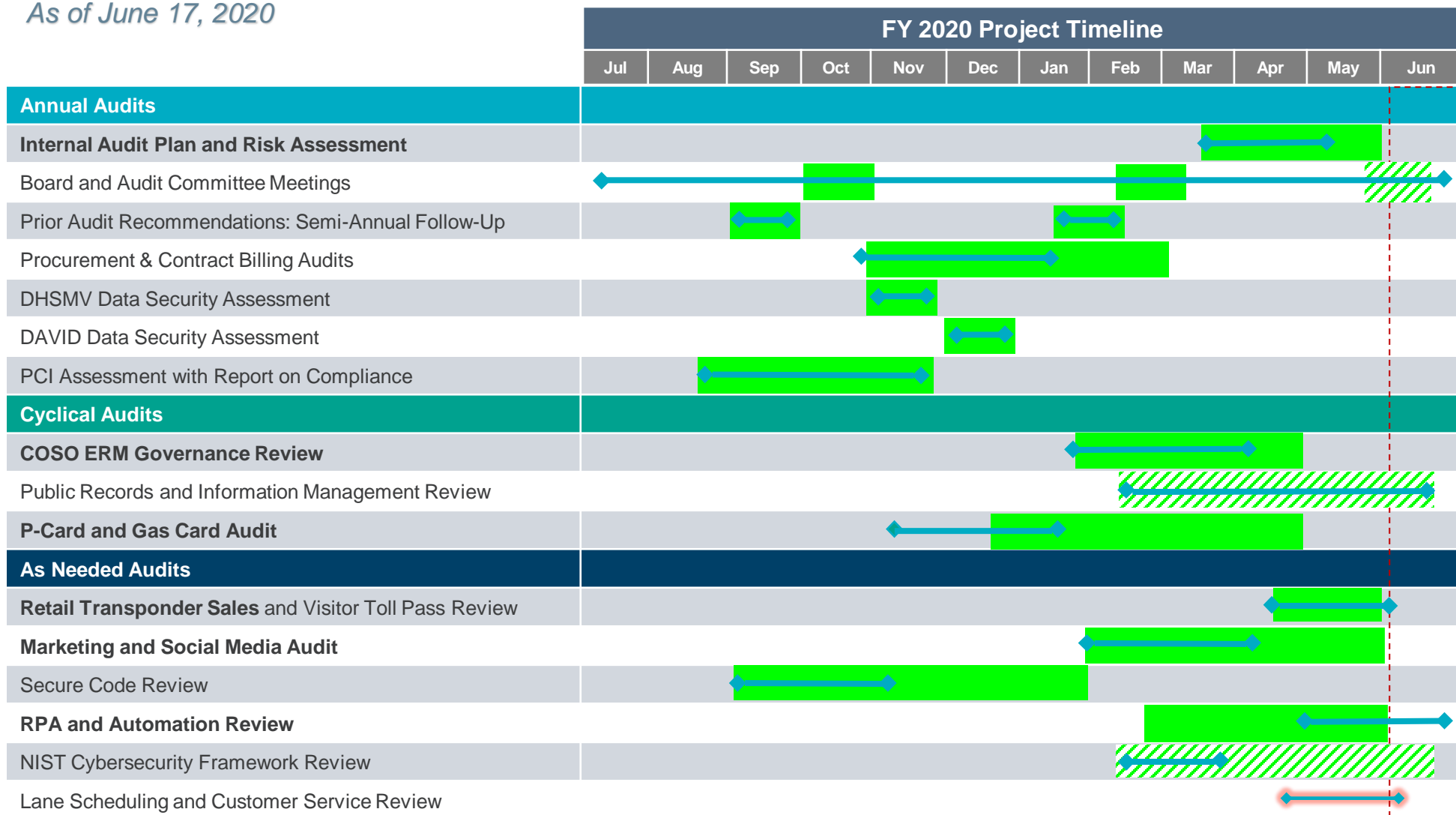
*Pursuant to the Florida Public Records Law and CFX Records Management Policy, audio tapes of all Board and applicable Committee meetings are maintained and available upon request to the Records Management Liaison Officer at [publicrecords@CFXway.com](mailto:publicrecords@CFXway.com) or 4974 ORL Tower Road, Orlando, FL 32807.*

# **D.1**

## **6-17-20 Status Update – Fiscal 2020 Internal Audit Plan**

# FY 2020 Internal Audit Dashboard

As of June 17, 2020



Plan  
 Cancelled  
 Complete  
 In-Process

**Bolded** projects have been completed since the March 2020 Audit Committee meeting

**D.2a**

**COSO ERM Governance  
Review**



# COSO ERM GOVERNANCE REVIEW

May 2020

**CENTRAL  
FLORIDA  
EXPRESSWAY  
AUTHORITY**

# TABLE OF CONTENTS

Section	Page
Executive Summary	3
Detailed Observations	7
Enhancement Opportunities	9
Appendix A – COSO 2013 Internal Control Framework	14
Appendix B – COSO 2017 Enterprise Risk Management Framework	22

# 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	<ul style="list-style-type: none"> <li>▪ Demonstrates a Commitment to Integrity and Ethical Values</li> <li>▪ Board Exercises Oversight Responsibility Over Internal Control</li> <li>▪ Management Establishes Structures, Authorities and Responsibilities</li> <li>▪ Demonstrates Commitment to Competence</li> <li>▪ Enforces Accountability</li> </ul>	21	0	N/A
Risk Assessment	<ul style="list-style-type: none"> <li>▪ Specifies Suitable Objectives</li> <li>▪ Identifies and Analyzes Risks</li> <li>▪ Assesses Fraud Risk</li> <li>▪ Identifies and Analyzes Significant Change</li> </ul>	25	0	N/A
Control Activities	<ul style="list-style-type: none"> <li>▪ Selects and Develops Control Activities</li> <li>▪ Selects and Develops General Controls over Technology</li> <li>▪ Deploys Controls through Policies and Procedures</li> </ul>	16	1	Moderate
Information & Communication	<ul style="list-style-type: none"> <li>▪ Uses Relevant Information</li> <li>▪ Communicates Internally</li> <li>▪ Communicates Externally</li> </ul>	22	0	N/A
Monitoring Activities	<ul style="list-style-type: none"> <li>▪ Conducts Ongoing and/or Separate Evaluations</li> <li>▪ Evaluates and Communicates Deficiencies</li> </ul>	10	0	N/A
TOTALS:		<b>94</b>	<b>1</b>	

# 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	<ul style="list-style-type: none"> <li>Exercise Board Risk Oversight</li> <li>Establishes Governance and Operating Model</li> <li>Defines Desired Organizational Behaviors</li> <li>Demonstrates Commitment to Integrity and Ethics</li> <li>Enforces Accountability</li> <li>Attracts, Develops, and Retains Talented Individuals</li> </ul>	1
Risk, Strategy, and Objective-Setting	<ul style="list-style-type: none"> <li>Considers Risk and Business Context</li> <li>Defines Risk Appetite</li> <li>Evaluates Alternative Strategies</li> <li>Considers Risk while Establishing Business Objectives</li> <li>Defines Acceptable Variation in Performance</li> </ul>	1
Risk in Execution	<ul style="list-style-type: none"> <li>Identifies Risk in Execution</li> <li>Assesses Severity of Risk</li> <li>Prioritizes Risks</li> <li>Identifies and Selects Risk Responses</li> <li>Assesses Risk in Execution</li> <li>Develops Portfolio View</li> </ul>	1
Risk Information, Communication, and Reporting	<ul style="list-style-type: none"> <li>Uses Relevant Information</li> <li>Leverages Information Systems</li> <li>Communications Risk Information</li> <li>Reports on Risk, Culture, and Performance</li> </ul>	1
Monitoring Enterprise Risk Management Performance	<ul style="list-style-type: none"> <li>Monitors Substantial Change</li> <li>Monitors Enterprise Risk Management</li> </ul>	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 Lombard, 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 Lombard, 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 Lombard, 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
<b>CONTROL ENVIRONMENT</b>	<ul style="list-style-type: none"> <li>• Demonstrates commitment to integrity and ethical values</li> <li>• Exercises oversight responsibility</li> <li>• Establishes structure, authority and responsibility</li> <li>• Demonstrates commitment to competence</li> <li>• Enforces accountability</li> </ul>	<p>4</p> <p>4</p> <p>3</p> <p>4</p> <p>5</p>
<b>RISK ASSESSMENT</b>	<ul style="list-style-type: none"> <li>• Specifies relevant objectives</li> <li>• Identifies and analyzes risk</li> <li>• Assesses fraud risk</li> <li>• Identifies and analyzes significant change</li> </ul>	<p>5</p> <p>5</p> <p>4</p> <p>3</p>
<b>CONTROL ACTIVITIES</b>	<ul style="list-style-type: none"> <li>• Selects and develops control activities</li> <li>• Selects and develops general controls over technology</li> <li>• Deploys through policies and procedures</li> </ul>	<p>6</p> <p>4</p> <p>6</p>
<b>INFORMATION &amp; COMMUNICATION</b>	<ul style="list-style-type: none"> <li>• Uses relevant information</li> <li>• Communicates internally</li> <li>• Communicates externally</li> </ul>	<p>5</p> <p>4</p> <p>5</p>
<b>MONITORING ACTIVITIES</b>	<ul style="list-style-type: none"> <li>• Conducts ongoing and/or separate evaluations</li> <li>• Evaluates and communicates deficiencies</li> </ul>	<p>7</p> <p>3</p>

# 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	<b>Risk Governance and Culture</b> - 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	<b>Risk, Strategy, and Objective-Setting</b> - 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	<b>Risk in Execution</b> - 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	<b>Risk Information, Communication, and Reporting</b> - 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	<b>Monitoring Enterprise Risk Management Performance</b> - 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*

© 2020 Protiviti Inc. All Rights Reserved. This document has been prepared for use by CFXs 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.

protiviti<sup>®</sup>

**D.2b**

**RPA and Automation  
Review**



# ROBOTIC PROCESS AUTOMATION REVIEW

Design Thinking and Idea Prioritization

# TABLE OF CONTENTS

Section	Page
Executive Summary	3
Design Thinking Summary	4
Design Thinking Results (RPA Candidates and ERP Considerations)	5 – 7



# EXECUTIVE SUMMARY



## Overview and Objectives

In accordance with the FY2020 Internal Audit Plan, Internal Audit led sessions and conducted interviews to enable a focused assessment of CFX's business and identify opportunities to apply Robotic Process Automation (RPA) to business processes that are manual, routine, repetitive, and time consuming in nature.



## Project Scope and Approach

As part of this review, Internal Audit performed the following:

1. Introduced RPA concepts to key stakeholders to understand the organization's state of maturity for leveraging process automation technology and to communicate the benefits of process automation;
2. Facilitated a design thinking session and conducted individual interviews to generate and capture ideas and prioritize manual business processes with potential for automation;
3. Aggregated and analyzed ideas to apply RPA to manual business processes based on value, suitability, and complexity to determine overall fit for process automation; and
4. Communicated additional process improvement insights and technology needs discovered through design thinking sessions and interviews.



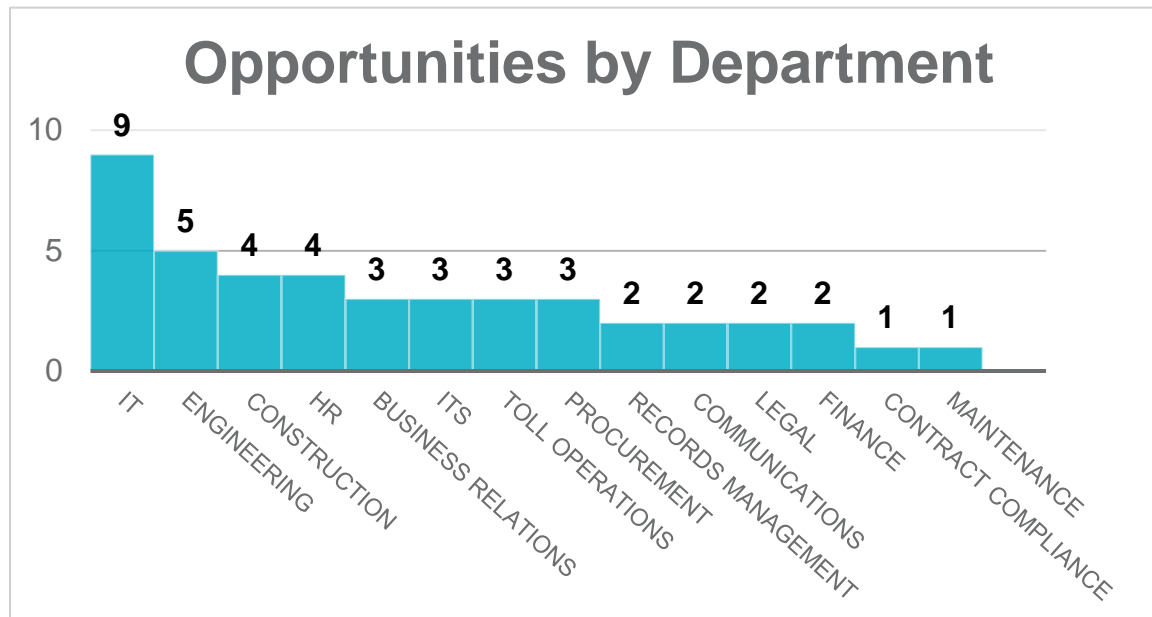
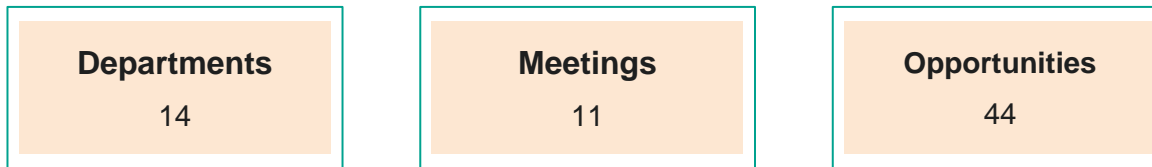
## Next Steps


Based upon the discussions held and opportunities identified, Protiviti will support requirements gathering for the procurement of a new ERP system as part of the fiscal 2021 internal audit plan. Subsequent to the ERP selection and in conjunction with development of future internal audit plans, Protiviti and CFX will consider the RPA candidates identified herein for future use case development and bot deployment.

# DESIGN THINKING SUMMARY

Protiviti planned and facilitated a group “design thinking” session and conducted individual interviews to foster idea generation and potential opportunities for process automation to improve the efficiency and/or effectiveness of CFX operations.

The potential opportunities identified were stratified into different buckets by potential solution. The opportunities for which RPA was deemed the ideal solution were further analyzed to prioritize and identify next steps. For many of the ideas and opportunities identified, the ideal solution was determined to be something other than RPA.



19 Design Thinking Participants 

44 Opportunities (Unique Ideas) Submitted 

11 RPA Candidates Identified 

10 Ideas for Future ERP Consideration 

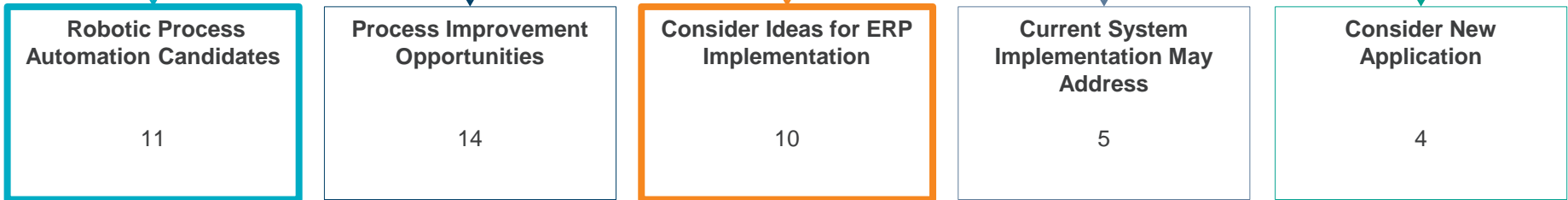
# DESIGN THINKING RESULTS

Design Thinking Session


Individual Interviews



44 Opportunities (Unique Ideas)



# ROBOTIC PROCESS AUTOMATION CANDIDATES

Identified for RPA Use Case	#	Process Name	Process Description	Process Owner	Value	Suitability	Complexity
	1	Monthly Interoperability Reconciliations	Reports from interoperable tolling agencies are manually reconciled to CFX internal reports each month.	Mike Carlisle	●	●	●
	2	CCTV Stream File Update	Periodic process to redistribute streaming access information to external partners.	Brent Poole	●	●	●
Other RPA Candidates	3	Cherwell Incident Management	Cherwell data exports must be manually imported into PowerBI daily to facilitate incident monitoring via PowerBI dashboards.	Maral Guerra-Torres	●	●	●
	4	Processing Unsubscribe Requests	Monthly process to unsubscribe customers from CFX communications involves substantial manual data entry from emails to Excel.	Maral Guerra-Torres	●	●	●
	5	Password Reset Requests	Password resets for certain systems require human approval. Approvals can only be performed manually through a laptop, which results in slower response times to requests made during non-business hours.	Maral Guerra-Torres	●	●	●
	6	User Access Review	User access for multiple applications is periodically reviewed for reasonableness.	Brent Poole	●	●	●
	7	Traffic Reporting	Traffic data reporting required by multiple users in the business is difficult to obtain and time consuming.	Jack Burch	●	●	●
	8	System Outage Diagnosis	Aggregation and root cause analysis for high volumes of ITS system outage notifications is manual and time consuming.	Brent Poole	●	●	●
	9	Law Enforcement Requests	Routine law enforcement records requests are time consuming to fulfill.	Tim O'Toole	●	●	●
	10	Citation Support Package	Preparing support package for citation enforcement involves running system reports and preparing spreadsheets manually.	Paul Schatz	●	●	●
	11	Upload Benefit Data to State Portal	Monthly process to manually upload approved employee benefits information to the State of Florida web portal.	Maral Guerra-Torres	●	●	●

# CONSIDER IDEAS FOR ERP IMPLEMENTATION

#	Process Name	Potential ERP Capability	Process Owner
1	Invoice Review Workflow	Automated workflow that routes invoices to appropriate personnel and tracks approval status.	Various
2	P-Card/Gas Card Review	Integrate with card providers to import transactions and implement approval workflow for electronic review. Implement application controls based on policy.	Carrie Baker
3	Automate Bank Reconciliation Spreadsheet	Banking integrations, rules, and bank reconciliation within ERP system.	Mike Carlisle
4	Approval Workflow for Purchase Orders	Automated workflow for purchase requisition through purchase order generation and delivery of the PO to the vendor.	Robert Johnson
5	Employees Update Data Changes (Address, etc.)	Self service system for employees to update information without assistance from HR.	Kendra Howard
6	Weekly Timesheets	Time reporting for hourly employees to reduce manual processes.	Kendra Howard
7	Automate New Hire Processes	Onboarding process workflow to automate key new hire steps.	Kendra Howard
8	Performance Reviews	Centralize and automate performance review process into standard electronic form with approval workflow.	Kendra Howard
9	Monthly Budget Tracker	Robust reporting to support detailed month-over-month budget to actual reports in Excel.	Fred Nieves
10	Budgeting Coordination	Requisition process and workflow for submitting expenditures for business relations through the marketing queue including improved process for expenditures and budget tracking.	Christie Seabury



Consider  
for ERP  
Solution

# *Face the Future with Confidence*

© 2020 Protiviti Inc. All Rights Reserved. This document has been prepared for use by CFXs 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.

protiviti®

**D.2c**

**P-Card and Gas Card  
Audit**



# PURCHASING CARD AND GAS CARD AUDIT

March 2020

**CENTRAL  
FLORIDA  
EXPRESSWAY  
AUTHORITY**



# TABLE OF CONTENTS

Section	Page
Executive Summary	3
Summary of Audit Procedures Performed and Results	4
Detailed Observations	6

# EXECUTIVE SUMMARY



## Overview

### Overview and Objectives

In accordance with the fiscal year 2020 Internal Audit Plan, Internal Audit reviewed the Central Florida Expressway Authority (“CFX”) Purchasing Card (P-Card) and Gas Card processes. CFX issues P-Cards and Gas Cards to employees for routine expenses. P-Cards and Gas Cards are to be used as outlined in the CFX Procurement Policy and Manual.

The objectives of this audit were to (1) identify and test key processes and internal controls within the P-card and Gas Card processes, (2) review selected transactions and activities for compliance with the CFX’s P-Card and Gas Card policies and procedures, and (3) propose recommendations, enhancements, and clarifications to strengthen CFX policies and internal controls.



## Project Scope and Approach

This audit was performed using a three-phased approach as outlined below:

### Phase I – Documentation of Current State Processes

Internal Audit interviewed management and reviewed existing policies and procedures in order to gain an understanding of key risks and controls related to the P-Card and Gas Card processes.

### Phase II – Review of Key Controls for Design and Operating Effectiveness

Internal Audit documented key controls relevant to the P-Card and Gas Card processes and evaluated the design effectiveness of the existing internal control structure. Following this evaluation, Internal Audit performed detailed procedures to review process infrastructure, card issuances, monitoring, spending review, deactivations, and other key attributes for each of the cards and related statements selected for audit. A summary of the procedures performed, results, and observations is provided on the following pages.

### Phase III – Reporting and Deliverables

Internal Audit prepared this report for management review and comment and issuance to the CFX Audit Committee.

# EXECUTIVE SUMMARY

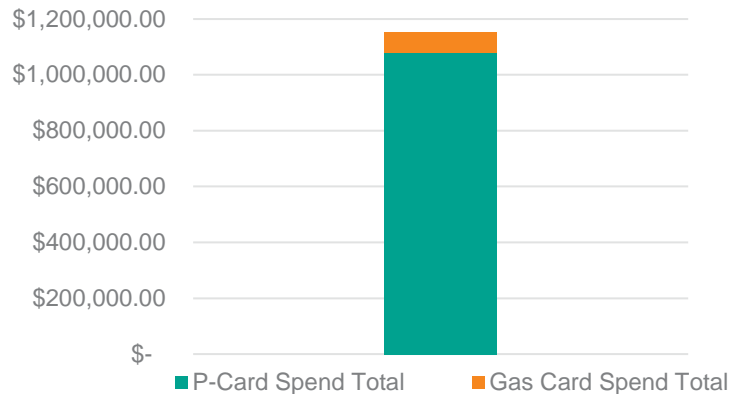


## Summary of Audit Procedures Performed and Results

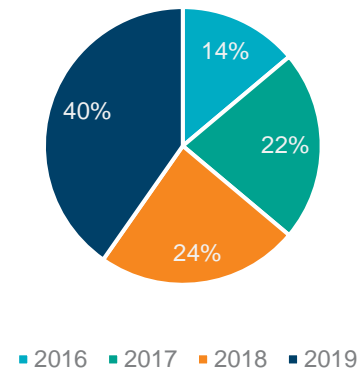
As of March 2020, the time of this audit, CFX had 49 active P-Cards and 19 active Gas Cards. P-Cards are used to cover qualified business-related expenses, such as training registrations and office supplies. Gas Cards are used to cover fuel expenditures related to CFX business travel. Internal Audit selected a period of three and a half years, July 1, 2016 – December 31, 2019, and conducted a review of the design and operating effectiveness of internal controls in place during this time frame. During the period of audit, CFX processed over 2,800 total P-Card and Gas Card statements and incurred over \$1.1M in total spend. As part of the internal control evaluation, Internal Audit selected 72 monthly statements consisting of 42 P-Card statements and 30 Gas Card statements for detailed spend transaction review. This detailed spend transaction review of 72 monthly statements covered \$55K in spend. Further detail on the total spend from July 1, 2016 – December 31, 2019 by card type, percentage of spend tested, and distribution of samples tested by year is summarized below:

Card Type	Population of Statements	Statements Tested	% of Statements Tested [1]	Total Spend During Testing Period	Total Spend Tested	% of Spend Tested [1]
P-Cards	2,058	42	2.04%	\$1,077,911	\$52,617	4.88%
Gas Cards	798	30	3.76%	\$72,233	\$2,162	2.99%

### Total Spend by Card Type



### Sample Distribution by Calendar Year



[1] Percentages are specific to statement and spend totals for each card type.

# EXECUTIVE SUMMARY



## Summary of Audit Procedures Performed and Results

The areas reviewed, audit observations, and related recommendations are outlined below:

Process	Key Areas Reviewed	Total Samples Tested	Number of Observations	Observation Reference	Relative Priority
Program Governance	Purchasing Card Manual, CFX procurement policies and procedures	-	2	1,2	<b>1 - High</b> <b>2 - Moderate</b>
Card Issuance	New card request documentation, card issuance authorization requirements, and card reissuance documentation	18	0	N/A	N/A
Card Monitoring	Internal card tracking logs, online banking and vendor portals, and physical card files	-	1	3	<b>3 - Moderate</b>
Spending Review	Monthly statement review, supporting documentation for incurred charges, authorization of significant charges, sales tax benchmarking and considerations	72	3	4, 5, 6	<b>4 - Moderate</b> <b>5 - Moderate</b> <b>6 - Moderate</b>
Card Deactivation	Bank and vendor portal logs of closed accounts, Human Resources listing of terminated employees, physically retained deactivated cards and documentation	12	0	N/A	N/A
<b>TOTALS:</b>		<b>102</b>	<b>6</b>		

# DETAILED OBSERVATIONS

# DETAILED OBSERVATIONS

## Observation 1 – P-Card and Gas Card Policies and Procedures

### Relative Priority

High

### Program Governance

### Card Issuance

### Card Monitoring

### Spending Review

### Card Deactivation

### Observation

The CFX P-Card Manual establishes procedures governing card issuance and deactivation, acceptable use, monthly spend monitoring, and consequences for noncompliance. However, the Manual contains outdated procedures and does not include documentation of the Contract Compliance Manager's quarterly audit process. For Gas Cards, no documented policy or procedure manual exists to govern issuances, deactivations, card changes, or spend monitoring processes at CFX.

Written policies and procedures are an integral component of the governance surrounding each critical business process. Policies and procedures provide guidance in the pursuit of achieving the objectives of the process, help reduce misunderstandings, and increase distribution of pertinent information to those involved in the process.

### Recommendation

Management should review and update the P-Card Manual to reflect current operating procedures, including consideration for the following:

- Procedures for the Contract Compliance Manager's quarterly compliance audit and follow-up actions for deviations identified.
- Policies regarding the appropriate use and storage of the P-Card for the main CFX bank account.
- Credit limit and monthly transaction limit authority matrix based on job title and required documentation for credit limit exceptions.
- Sales tax exemption process updates including a new exception process in which employees must seek prior approval for and substantiate taxed purchases as more economical than a tax-exempt alternative.

Management should develop a comprehensive Gas Card policy and procedure manual including the following features:

- Clearly defined responsibilities and requirements for Gas Card issuance, monitoring, spending review, and deactivation.
- Appropriate use of Gas Cards, such as limiting cards for fuel expenditures only, with no maintenance spending permitted.
- Procedures for tracking pooled vehicle use, monitoring expenditures, and documenting responsible employees for charges incurred.

# DETAILED OBSERVATIONS

## Observation 1 – P-Card and Gas Card Policies and Procedures (continued)

### Relative Priority

High

### Management Response

Management concurs.

### Management Action Plan

Management will update the Procurement Policy to incorporate a Gas Card policy. Management will update the P-Card Manual to reflect current procedures as recommended and will develop Gas Card procedures to supplement the documentation set.

### Action Plan Owner / Due Date

Aneth Williams, Director of Procurement / December 31, 2020

Program  
Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation

# DETAILED OBSERVATIONS

## Observation 2 – Digital Workflow Opportunities

### Relative Priority

Moderate

### Program Governance

### Card Issuance

### Card Monitoring

### Spending Review

### Card Deactivation

### Observation

To appropriately record P-Card and Gas Card issuance, reissuance, and deactivation, request forms are circulated manually for various approvals and maintained in paper form by the Program Administrator. Through control testing, the following process and documentation inconsistencies were identified:

- a. For all ten **new card issuances** tested, Division Chief approval was not documented on the request form;
- b. All five **card deactivations** tested were processed without a request form and documented approvals;
- c. For all 14 **card re-issuances** due to card expiration or card security concerns that were tested, the re-issuances were processed without a request form and documented approvals;
- d. For the new card issuances tested, employee acknowledgement of P-Card and Gas Card policies and completion of training was inconsistently documented through varying forms and language.

### Recommendation

CFX would benefit from more standardization in its process and the implementation of a digital workflow. A digital workflow would help CFX achieve greater consistency in the execution of internal controls and enhance the overall maturity of the P-Card and Gas Card issuance and deactivation processes.

Specifically, CFX should consider transitioning the following manual processes to a digital workflow by leveraging SharePoint or another available technology:

- Card issuance and re-issuance requests and approvals
- Card deactivation requests and approvals
- Employee acknowledgement of key policies, training, and receipt of P-Cards and Gas Cards
- Advance approvals for significant purchases
- Advance approvals and documentation of transactions with sales tax



# DETAILED OBSERVATIONS

## Observation 2 – Digital Workflow Opportunities (continued)

### Relative Priority

Moderate

### Program Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation

### Management Response

Management concurs.

### Management Action Plan

Procurement will work with the IT team to determine the best workflow option for each part of the recommendation (Adobe Sign, SharePoint, or others). Management will develop and implement the digital workflow(s) in accordance with the recommendation.

### Action Plan Owner / Due Date

Aneth Williams, Director of Procurement / December 31, 2020

# DETAILED OBSERVATIONS

## Observation 3 – Monitoring of Active Cards

### Relative Priority

Moderate

Program  
Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation

### Observation

Active card rosters for P-Cards and Gas Cards are not reviewed on a periodic basis for appropriateness by an individual other than the Program Administrator. Lack of periodic review of employees with active P-Cards or Gas Cards elevates the risk of improper use or unauthorized spending.

### Recommendation

Active cards per the issuer online portals should be reviewed on a semi-annual basis by the Chief Financial Officer. The CFO should adopt the following procedures for this review:

- 1) Reconciliation of open cards in the card issuer online portals to the active employee roster to review for terminated employees,
- 2) Reconciliation of Pool Vehicle Gas Cards to vehicles in use and to verify the assigned custodian is appropriate and documented for each Gas Card,
- 3) Review for existence of more than one active card for an individual employee, and
- 4) Review credit/transaction limits for appropriateness based on job title and role.

### Management Response

Management concurs.

### Management Action Plan

Management will implement a review of active card users to be performed twice per year by the CFO.

### Action Plan Owner / Due Date

Lisa Lumbard, Chief Financial Officer / June 30, 2020

# DETAILED OBSERVATIONS

## Observation 4 – Pool Vehicle Gas Cards

### Relative Priority

Moderate

Program  
Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation

### Observation

CFX maintains four Pool Vehicles and four associated Gas Cards for shared business use. The following processes to manage Pool Vehicles and review monthly Gas Card spend can be enhanced to reduce CFX's risk of card theft or misuse:

1. Gas Cards are stored within each Pool Vehicle along with the Gas Card PIN number.
2. The keys for the Pool Vehicles are maintained by administrative employees, giving these administrative employees unrestricted access to the vehicles, Gas Cards, and PIN numbers.
3. The tracking process for employee use of Pool Vehicles and Gas Cards is inconsistently performed for the four Pool Vehicles.
4. Within the Gas Card transactions tested, four transaction receipts were not signed by an employee to document responsibility and one transaction was not supported by a receipt.

Appropriate segregation of duties, tracking of assets, and documentation may help CFX enhance accountability for spending, enforce policies, and identify inappropriate charges.

### Recommendation

Management should consider the following process improvements for Pool Vehicles and related Gas Cards:

- To reduce the risk of theft and misuse, Gas Cards should not be stored in Pool Vehicles.
- One tracking log should be created for each Pool Vehicle to track vehicle use and enable the assignment of responsibility for Gas Card charges. The tracking logs should be provided to the Procurement Department for review and retention with the monthly Gas Card statements.
- During the monthly spending review for each Pool Vehicle Gas Card, a detailed analysis should be performed between tracking logs and Gas Card statements to assign and document the employee responsible for each charge. This procedure may help detect fraudulent charges if a charge was incurred when the vehicle was not checked out to an employee.

# DETAILED OBSERVATIONS

## Observation 4 – Pool Vehicle Gas Cards (continued)

### Relative Priority

Moderate

Program  
Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation

### Management Response

Management concurs.

### Management Action Plan

Management will remove the Gas Cards from the Pool Vehicles and will implement a standard tracking log to be used consistently for all Pool Vehicles. Management will improve the monthly review of Gas Card spend through use of the tracking logs to assign and document the employee responsible for each charge.

### Action Plan Owner / Due Date

Lisa Lumbard, Chief Financial Officer / July 31, 2020

# DETAILED OBSERVATIONS

## Observation 5 – ERP Integration

### Relative Priority

Moderate

Program Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation

### Observation

Per CFX's P-Card Manual, all charges incurred must be supported by original receipts, each P-Card statement must be signed by the cardholder's supervisor and Program Administrator as evidence of review, and all charges exceeding Procurement Level 1 (\$999.99) require prior approval from the Program Administrator.

Through detailed P-Card statement testing, the following instances of noncompliance with CFX's P-Card Manual were identified:

1. For two of 42 samples tested, charges were not supported by receipts and a Lost Receipt Form was not completed.
2. For three of 42 samples tested, approvals from either the employee's supervisor or the Program Administrator were not documented to show evidence of the required review.
3. For seven of nine charges exceeding \$999.99, advance approval from the Program Administrator was not documented or retained with the P-Card statement.

Inconsistency in reviews and approvals and evidence of such may result in inappropriate purchases remaining undetected.

### Recommendation

As procurement criteria are defined in conjunction with CFX's new ERP, CFX should consider the opportunity to integrate P-Card transaction data. A digital workflow and integration of P-Card transactions may assist CFX with consistent documentation retention and approval evidence in accordance with the P-Card Manual.

In the interim, to help create more consistency with managing lost receipts and appropriate levels of review and approval, each cardholder's supervisor and Program Administrator should sign off on a checklist documenting review responsibilities, a completeness check for receipts and completion Lost Receipt Forms, and advance approval for purchases exceeding Procurement Level 1. The Contract Compliance Manager's quarterly audit checklist can be leveraged as a basis for creating this review checklist.

For spending in excess of Procurement Level 1, implementation of a digital workflow could be leveraged to support consistency and documentation of advance approvals for significant purchases.

# DETAILED OBSERVATIONS

## Observation 5 – ERP Integration (continued)

### Relative Priority

Moderate

### Management Response

Management concurs.

### Management Action Plan

Management will develop a checklist for supervisors to be used during their monthly review of P-Card transactions. P-Card/Gas Card integrations and process improvements will be included in the ERP requirements during RFP development.

### Action Plan Owner / Due Date

Aneth Williams, Director of Procurement / September 30, 2020

Program  
Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation

# DETAILED OBSERVATIONS

## Observation 6 – Quarterly Audit

### Relative Priority

Moderate

Program  
Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation

### Observation

The Contract Compliance Manager performs a quarterly P-Card compliance audit which includes a review of all P-Card monthly statements and transactions and re-performance of the Program Administrator's monthly review to identify any deviations from policy as outlined in the CFX P-Card Manual.

During the testing period, the quarterly review process was not completed in a timely manner due to the level of detail necessary and volume of transactions involved. Additionally, the current P-Card vendor does not provide CFX with access to consolidated P-Card transaction data in Excel or other digital format. Access to digital transaction data would help speed up the quarterly audit and enable CFX to take a more risk-based approach to detect errors or fraudulent charges.

### Recommendation

CFX should coordinate with the P-Card vendor to seek transaction data in a digital format such as Excel. Having consolidated transaction data in a digital format would facilitate risk-based sampling for the P-Card compliance audit rather than auditing entire populations of data, thus making the process more efficient, and also enable CFX to perform basic data analytics each quarter.

If CFX is successful at obtaining P-Card transaction data in a digital format, CFX should update its quarterly P-Card compliance audit process to incorporate a more risk-based approach. In doing so, CFX may consider incorporating the following guidelines for conducting quarterly audits:

1. Audit at least ten percent coverage of total spend per quarter
2. Audit P-Cards and employees with the largest spend per quarter
3. Review data for abnormally large P-Card spend and audit large transactions
4. Audit all transactions exceeding Procurement Level 1 (\$999.99)
5. Apply other data analytical procedures to detect potential fraud or abuse
6. Review for deactivated card and terminated employee use

# DETAILED OBSERVATIONS

## Observation 6 – Quarterly Audit (continued)

### Relative Priority

Moderate

### Management Response

Management concurs.

### Management Action Plan

Management will review P-Card vendor reporting capabilities to extract transaction data. The Manager of Contract Compliance will implement a process to review transaction data and sample P-Card monthly statements for the quarterly audit. Procedures will be updated as the process is developed.

### Action Plan Owner / Due Date

Carrie Baker, Manager of Contract Compliance / October 31, 2020

Program  
Governance

Card Issuance

Card Monitoring

Spending Review

Card Deactivation



*Face the Future with Confidence*

© 2020 Protiviti Inc. All Rights Reserved. This document has been prepared for use by CFXs 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.

protiviti®

# **D.2d**

## **Retail Transponder Sales Review**



# RETAIL TRANSPONDER SALES REVIEW

May 2020

**CENTRAL  
FLORIDA  
EXPRESSWAY  
AUTHORITY**

# TABLE OF CONTENTS

Section	Page
Executive Summary	3
Summary of Audit Procedures Performed and Results	4
Detailed Observations	5

# EXECUTIVE SUMMARY



## Project Overview, Scope, and Approach

### Overview

In accordance with the fiscal year 2020 Internal Audit Plan, Internal Audit reviewed the policies and procedures surrounding Central Florida Expressway Authority (“CFX”) marketing of E-PASS transponders through various sales channels and the related management of transponder physical inventory. This audit had not been performed previously for CFX.

As part of its strategy to increase the number of E-PASS customers, CFX operates a retail transponder program whereby E-PASS transponders are marketed and distributed through university bookstores throughout Florida and via consignment through Amazon. CFX currently sells branded CollegePass sticker transponders to the bookstores and consigns E-PASS portable transponders with Amazon.

Details on the retail transponder program are below. Data is through May 31, 2020, was obtained from CFX, and is for informational purposes only:

CollegePass Brand	Retail Program Launch	Retail Transponder Sales (Launch – May 31, 2020)
GatorPass	August 2017	344
NolePass	August 2017	250
KnightPass	November 2017	350

Amazon Program Launch	Transponders Consigned to Amazon (Launch – May 31, 2020)	Amazon Transponder Sales (Launch – May 31, 2020)
August 2018	2,370	2,100

### Project Scope and Approach

The objectives of this audit were to (1) identify key processes and internal controls around retail transponder sales and inventory management, (2) review key controls for design effectiveness, (3) perform limited procedures to evaluate selected transactions for operating effectiveness, and (4) propose recommendations, enhancements, and clarifications to strengthen CFX policies and internal controls. Details of the procedures performed, results, and observations are provided in the body of this report.

# EXECUTIVE SUMMARY



## Summary of Audit Procedures Performed and Results

The areas reviewed, audit observations, and relative priority are outlined below:

Process	Key Areas Reviewed	Total Controls Tested	Number of Observations	Observation Reference	Relative Priority
Process Governance	Policies and procedures, system capabilities and reporting	1	2	1, 2	1 – High 2 – Moderate
Inventory Management	Order management, receiving, recording, physical counts, reconciliations	5	1	3	3 – Low
Retail Sales & Distribution	Contract terms and approvals, order fulfillment, transponder and account analytics	4	1	4	4 – Low
Accounting & Finance Processes	Purchase order approval, invoice processing, financial reporting	2	-	-	-
TOTALS:		12	4	-	-

# DETAILED OBSERVATIONS

# DETAILED OBSERVATIONS

## Observation 1 – Inventory Management System

### Relative Priority

High

### Process Governance

### Inventory Management

### Retail Sales & Distribution

### Accounting & Finance

### Observation

TRIMS is the existing customer relationship management (CRM) system. Due to certain limitations within TRIMS, current processes to manage retail transponder inventory and the related financial transactions are manual and heavily reliant on spreadsheets. The current, manual processes in place to manage transponder inventory help reduce the risk of transponder misappropriation and inaccurate recording of retail sales. To further mature the inventory management process, system capabilities could be improved to better support business needs and improve efficiency in the following areas:

- No system capability exists to record and track physical transponder inventory by transponder type, sales channel, and location (e.g. on-site storage vs. consignment). As a result, transponder inventory is maintained manually through spreadsheets, which draw from multiple, disparate data sources. Additionally, some inventory information is maintained separately by both the Toll Operations and Finance Departments.
- No system capability exists to record transponders sold or consigned but not yet activated. Additionally, the system does not support a wider variety of transaction types (e.g. sales, exchanges, transfers, giveaways) or segregate sales by channel (bookstore vs. consignment). Consequently, sales and cost of goods sold are calculated manually using multiple sources of information and are subject to estimation.
- Although several custom reports exist to capture new accounts and transponder activations through certain channels, no comprehensive reporting exists to support critical marketing reporting across all relevant data points.

### Recommendation

Management should form a working group to consider the system capabilities and reporting needs related to retail transponder sales in the areas of inventory management, financial reporting, and marketing reporting. System and reporting needs identified should be explored with the CRM implementation project team to determine if needs can be met by the new CRM system or add-on modules. If needs cannot be met by the new CRM system, management should consider additional alternatives, including the cost/benefit of a new, off-the-shelf application or a custom application to support inventory management, financial reporting, and marketing reporting.



# DETAILED OBSERVATIONS

## Observation 1 – Inventory Management System (continued)

### Relative Priority

High

### Management Response

Management concurs.

### Management Action Plan

CFX will organize a working group comprised of stakeholders involved in retail transponder sales and inventory management processes and IT to discuss fulfillment of key reporting needs through current CRM implementation.

### Action Plan Owner / Due Date

Mike Carlisle, Director of Accounting and Finance / March 31, 2021

### Process Governance

Inventory Management

Retail Sales &  
Distribution

Accounting & Finance

# DETAILED OBSERVATIONS

## Observation 2 – Procedural Documentation

### Relative Priority

Moderate

### Process Governance

### Inventory Management

### Retail Sales & Distribution

### Accounting & Finance

### Observation

Opportunity exists to enhance the current procedural documentation that guides CFX's inventory management practices and its retail transponder sales. Written procedures are an integral component of the infrastructure surrounding each critical business process. Procedures 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.

### Recommendation

Management should update procedural documentation specific to retail transponder sales and inventory management practices to include the following:

- Receipt and recording of purchase orders from retailers
- Reconciliation of goods ordered, invoiced, and shipped
- Recording of inventory transactions; reconciliation of inventory to records
- Recording of significant journal entries (sales revenue, cost of sales, inventory adjustments)

### Management Response

Management concurs.

### Management Action Plan

Management will review all inventory management and transponder sales documentation (including retail sales) to ensure all procedures are adequately documented.

### Action Plan Owner / Due Date

Mike Carlisle, Director of Accounting and Finance; Angela Melton, Manager of Communications; Fred Nieves, Manager—E-Pass and Plaza Operations / December 31, 2020

# DETAILED OBSERVATIONS

## Observation 3 – Inventory Data Access

### Relative Priority

Low

Process Governance

Inventory Management

Retail Sales &  
Distribution

Accounting & Finance

### Observation

As leading practice, an organization should ensure that access to folders containing significant spreadsheets is restricted to appropriate personnel. Currently, key transponder inventory data that is used by Operations to manage inventory levels resides in an Excel spreadsheet on a shared drive. Finance maintains separate inventory records and relies on separate counts to confirm accuracy of balance sheet inventory values. The operational spreadsheet is stored within a folder accessible to all members of the E-Pass back office staff. Although the operational inventory spreadsheet is primarily maintained and managed by only two members of the E-Pass back office staff, several dozen other contractor employees possess the ability to modify the file. Without proper access restriction, key operational transponder inventory data could be lost or overwritten.

### Recommendation

Management should perform a review of access to folders containing significant spreadsheets within the Toll Operations Department to ensure access is appropriate based on role and job responsibility.

### Management Response

Management concurs.

### Management Action Plan

Management will perform a review of access to key operational spreadsheets by the established due date in either the system folders or SharePoint depending on the status of the SharePoint migration.

### Action Plan Owner / Due Date

Fred Nieves, Manager—E-Pass and Plaza Operations / August 31, 2020

# DETAILED OBSERVATIONS

## Observation 4 – Transponder Shipping

### Relative Priority

Low

Process Governance

Inventory Management

Retail Sales & Distribution

Accounting & Finance

### Observation

As transponder orders are received from retail partners, they are forwarded to Toll Operations for fulfillment. A list is compiled as transponders are packed by Toll Operations. The compiled list and box of transponders are given to the Manager of Communications for verification. Prior to shipping, the Manager of Communications performs a physical reconciliation between the order from the retail partner, the physical transponders packed for shipment, the list of transponders provided by Toll Operations, and the invoice prepared by Finance. Based on the current process, shipping and order fulfillment responsibilities for retail transponders are shared between Toll Operations and Communications, which does not align with the strategic objectives of the departments, creates inefficiencies in the process, and is inconsistent with CFX's direct-sales transponder order fulfillment process.

### Recommendation

Management should consider realigning fulfillment and shipping responsibilities to Toll Operations to create more consistency in execution and oversight of the process. As management realigns responsibilities, documentation of the reconciliation between transponders ordered, transponders prepared for shipment, and transponders invoiced, including evidence of approval for the shipment, should be retained. This reconciliation should be performed prior to shipment and by someone not involved in the packing of transponders.

### Management Response

Management concurs.

### Management Action Plan

Management will consider realignment of the order fulfillment and shipping function for the retail program as recommended. As realignment is considered, management will also develop documentation requirements for each retail shipment that includes evidencing the reconciliation between the original order, the shipping manifest verified by physical count of transponders, and the invoice prepared by Finance.

### Action Plan Owner / Due Date

Lisa Lombard, Chief Financial Officer / December 31, 2020

# *Face the Future with Confidence*

© 2020 Protiviti Inc. All Rights Reserved. This document has been prepared for use by CFXs 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.

protiviti<sup>®</sup>

**D.2e**

**Marketing and Social  
Media Audit**



# MARKETING AND SOCIAL MEDIA AUDIT

March 2020

**CENTRAL  
FLORIDA  
EXPRESSWAY  
AUTHORITY**

# TABLE OF CONTENTS

Section	Page
Executive Summary	3
Summary of Audit Procedures Performed and Results	5
Summary of Peer Benchmarking Results	6
Enhancement Opportunities	7



# EXECUTIVE SUMMARY



## Overview

### Overview

In accordance with the fiscal year 2020 Internal Audit Plan, Internal Audit reviewed the policies and procedures surrounding Central Florida Expressway Authority (“CFX”) social media management and communication plan. This audit has not been performed previously for CFX.

CFX began using social media on a frequent basis after the statewide centralized customer service system (CCSS) was put in place to support SunPass toll collections. CFX has its own back office and brand, E-PASS, and is not part of the statewide CCSS. In order to effectively respond to CFX customer issues relating to the SunPass system that began in 2018, such as backlogged tolls, billing questions, and long customer service wait times, CFX began a program to leverage social media to respond timely to customer inquiries and to differentiate its brand during a difficult time in SunPass tolling. CFX has continued to be progressive in its use of certain social media platforms for branding purposes, customer outreach initiatives, and to provide an avenue for customers to contact the agency.

CFX procures consulting services from the following outside vendors as part of the social media management process:

1. Day Communications for Public Outreach Education and Communications Consultant Services, which includes assisting with CFX’s overall goal to increase community reach through social media platforms and social media strategy development.
2. Doverwood Communications as an approved subcontractor to the Day Communications contract. Doverwood provides social media subject matter expertise to support Day Communications in the services being provided to CFX.

CFX and its consultants utilize three platforms to manage its social media communications via a variety of channels, including Twitter, Instagram, and Facebook. The three management platforms are Hootsuite and Sprout Social as general social media management and scheduling tools, and Basecamp as a project management tool. CFX maintains the accounts with Hootsuite and Spout Social; however, the Basecamp application is owned by Day Communications.

### Objectives

The objectives of this audit were to (1) Evaluate CFX’s social media management practices, including the management of CFX communication, social media risks, and internal controls, and (2) Compare CFX’s social media management practices to other organizations of similar complexity for opportunities to adopt leading practices.

# EXECUTIVE SUMMARY



## Project Scope and Approach (Continued)

This audit was performed using a three-phased approach as outlined below:

### Phase I – Documentation of Current State Social Media Management Process

Internal Audit documented the current state of social media management and communication processes through interviews with key management personnel and review of existing policies and procedures.

### Phase II – Comparison of Social Media Management Process to Peers

Internal Audit performed a benchmarking comparison of CFX's social media strategies and key controls against those of four peers, including three tolling agencies and one private company in order to identify opportunities for improvement and further understand level of maturity in the CFX social media process.

### Phase III – Assessment and Test of Key Controls for Design Effectiveness

Internal Audit reviewed CFX's processes, policies, and procedures related to social media management against Protiviti's leading practice framework of eight social media risk management processes. Key internal controls within each risk area were identified and tested. A summary of the procedures performed, results, and observations are provided on the following pages.

#### The Eight Core Social Media Risk Management Processes

Develop and Communicate Strategy – *Social media plan aligned with CFX strategy*

Sustain Leadership – *High-level governance and oversight exercised over program and policies*

Promote Culture – *Policies and training support awareness, participation, exposure, and alignment*

Manage Community – *Processes and procedures govern incident response, marketing, and community outreach*

Refresh Content and Programming – *Sharing and posting of information follows a managed process*

Enforce Policies and Governance – *Policies govern acceptable use, security, and risk management*

Deploy Tools – *Processes guide management of tools/platforms*

Measure and Report – *Monitoring of key metrics supports evaluation of results and drives strategy*

# EXECUTIVE SUMMARY



## Summary of Procedures and Results

Core Risk	Key Areas Reviewed	Total Controls Tested	Number of Opportunities	Opportunity Reference	Relative Priority
Develop and Communicate Strategy	Marketing campaign strategy and social media impact	2	-	-	-
Sustain Leadership	Senior leadership involvement in social media processes	1	-	-	-
Promote Culture	Internal social media processes; Employee, contractor, and vendor policies; Social media training and awareness	3	1	1	1 - Moderate
Manage Community	Selection of appropriate platforms; Platform access restrictions; Social media communication monitoring; Social media incident response	4	-	-	-
Refresh Content and Programming	Social media procedures and brand management	3	-	-	-
Enforce Policies and Governance	Review of social media management, policies and procedures; Legal and compliance implications; Access to sites and security	6	3	2, 3, 4	2 - Moderate 3 - Moderate 4 - Low
Deploy Tools	Social media tools and change management; Vendor involvement and contracts	4	-	-	-
Measure and Report	Social media metrics and reporting	1	-	-	-
TOTALS:		24	4	-	-

# EXECUTIVE SUMMARY



## Summary of Peer Benchmarking Results

The following benchmarking comparison was created to depict CFX's social media process maturity against those of four peers. Internal Audit performed inquiry with Peers 1-3, which are comparable in size and/or industry to CFX. Peer 4 is a large, Central Florida-based company with a significant social media presence and prevalence in the local community. No testing outside of inquiry was performed over any peer group. The peer benchmarking was considered in developing opportunities for CFX to consider to enhance the maturity of its social media program.

Topic	CFX	Peer 1	Peer 2	Peer 3	Peer 4
Size of Company / Employees in Social Media	80 employees / 3 social media employees (1 open position)	6,500 employees / 2 social media employees	Fewer than 100 employees / 3 social media employees	50 employees / 3 social media employees	20,000+ employees / 8+ social media employees
Social Media Vendor/Consultant	X	X		X	
Additional Social Media Platforms Used (Other than Twitter, Instagram, Facebook, and YouTube)			LinkedIn		Snapchat, Pinterest
Senior Management Involvement	X				X
Employee Social Media Use Policy	X	X		X	X
Contractor Social Media Use Guidelines			X		
Social Media Refresh Acknowledgement			None		
Social Media Incident Response Procedure		X			
Social Media Process Manual	X	X			X
Anti-Virus and Anti-Malware Software Use	X	X	X	X	X
Reporting and Metrics	X		X	X	X

# ENHANCEMENT OPPORTUNITIES

# ENHANCEMENT OPPORTUNITIES

## Opportunity 1 – Social Media Use Guidelines and Awareness

### Relative Priority

Moderate

Deploy and Communicate Strategy

Sustain Leadership

Promote Culture

Manage Community

Refresh Content and Programming

Enforce Policies and Governance

Deploy Tools

Measure and Report

### Observation

Based on the framework of leading practices, the organization should set clear social media use guidelines that are easily accessible to all contractors and employees and should develop periodic internal training programs for employees to promote awareness of policies.

A risk point for CFX is uncontrolled social media use by CFX contractors and their employees that impacts CFX reputation and image. As a result, there is an opportunity to create a separate social media use guideline or policy specific to contractors.

In addition, CFX employees are trained on social media use policies during onboarding, however periodic refresh training or annual acknowledgement of social media use policies is not performed. Continuing education training is not provided annually for employees involved in managing social media for CFX.

Clear contractor policies/guidelines and employee awareness help prevent inappropriate social media use, which could present reputational risk to the organization.

### Recommendation

Management should develop a social media use guideline or policy for CFX contractors and subcontractors to help mitigate potential reputational risk. The following areas can be considered when developing social media use guidelines for contractors and their employees:

- Prohibiting use of CFX brand, name, logo including portrayal as employees of CFX, on social media platforms;
- Prohibiting photos/posting while on CFX premises, in CFX uniform, or while conducting CFX business;
- Usage of social media during crisis situations; and
- Frequently Asked Questions for contractor/subcontractor employees.

Additionally, management should incorporate an annual social media policy acknowledgement for all CFX employees and should implement periodic social media continuing education for employees that work directly with social media platforms and tools.

# ENHANCEMENT OPPORTUNITIES

## Opportunity 1 – Social Media Use Guidelines and Awareness (continued)

### Relative Priority

Moderate

Deploy and Communicate Strategy

Sustain Leadership

Promote Culture

Manage Community

Refresh Content and Programming

Enforce Policies and Governance

Deploy Tools

Measure and Report

### Management Response

Management concurs.

### Management Action Plan

Management will develop a social media use guideline or policy for CFX contractor and subcontractor employees. Management will also incorporate an annual social media policy acknowledgement for all CFX employees. Finally, management will implement periodic social media continuing education for employees that work directly with social media platforms and tools.

### Action Plan Owner / Due Date

Michelle Maikisch, Chief of Staff/Public Affairs Officer / June 30, 2021

# ENHANCEMENT OPPORTUNITIES

## Opportunity 2 – Password Policy and User Access Provisioning

### Relative Priority

Moderate

Deploy and Communicate Strategy

Sustain Leadership

Promote Culture

Manage Community

Refresh Content and Programming

Enforce Policies and Governance

Deploy Tools

Measure and Report

### Observation

As leading practice, social media password parameters and internal controls should comply with CFX IT Policy for overall IT security governance. CFX IT Policy states that passwords should contain at least 8 characters, including a combination of letters, numbers, and special characters, should be changed every 90 days, and should not be shared. In addition, passwords should not be stored in written form unless secured in an approved manner.

Internal Audit identified that password management practices for social media platforms and tools did not conform to leading practice and CFX IT Policy in the following ways:

1. Complexity and rotation;
2. Passwords for social media sites and tools are shared among users; and
3. Passwords are stored in written form in an Excel file.

Strong password controls help prevent security breaches and information loss that could damage reputation.

### Recommendation

Management should review social media platform and tool capabilities against CFX IT Policy to better align social media password controls with the organization's overall IT security strategy. Management should work with IT to align social media passwords to CFX IT Policy where possible.

Management should consider the following areas for improvement across all social media platforms and tools, where supported:

- Revise social media passwords and the ongoing password management process to conform with the complexity and password modification requirements defined in CFX's IT Policy;
- Eliminate the sharing of passwords by creating separate user credentials within Sprout Social and Hootsuite, where possible;
- Establish a standard approval and documentation process to provision and deprovision user access for social media employees and consultants;
- Implement use of a password vault to store and retrieve social media passwords; and
- As a leading practice, incorporate a dual-factor authentication to access social media sites and applications for all provisioned users.



# ENHANCEMENT OPPORTUNITIES

## Opportunity 2 – Password Policy and User Access Provisioning (continued)

### Relative Priority

Moderate

Deploy and Communicate Strategy

Sustain Leadership

Promote Culture

Manage Community

Refresh Content and Programming

Enforce Policies and Governance

Deploy Tools

Measure and Report

### Management Response

Management concurs.

### Management Action Plan

Management will review the recommendation and work collaboratively to develop an approach that improves social media password and user access provisioning controls and aligns with CFX and social media capabilities.

### Action Plan Owner / Due Date

Michelle Maikisch, Chief of Staff/Public Affairs Officer, and Jim Greer, Chief of Technology and Operations / January 31, 2021

# ENHANCEMENT OPPORTUNITIES

## Opportunity 3 – User Access Review

### Relative Priority

Moderate

Deploy and Communicate Strategy

Sustain Leadership

Promote Culture

Manage Community

Refresh Content and Programming

Enforce Policies and Governance

Deploy Tools

Measure and Report

### Observation

Based on the social media framework of leading practices, an organization should ensure that access is appropriately restricted to social media sites and a periodic review of user access should be performed by an employee that is independent of the user administration role.

Not performing periodic review of user access may increase the risk of inappropriate access to social media accounts, which presents a reputational risk to CFX due to the connection the accounts provide to the community.

### Recommendation

Upon completion of the management action plans to provision and deprovision user access in Sprout Social and Hootsuite or other third-party social media management tool, management should implement a periodic process to generate a user listing from the applications and perform an independent review of the user access list for appropriateness.

For other social media platforms not managed by a third-party social media management tool (such as Instagram), management should independently review users with access in conjunction with the third-party social media management tool user listing reviews.

### Management Response

Management concurs.

### Management Action Plan

Management will establish and document a periodic independent review of social media user access lists across all social media tools or platforms.

### Action Plan Owner / Due Date

Michelle Maikisch, Chief of Staff/Public Affairs Officer / December 31, 2020

# ENHANCEMENT OPPORTUNITIES

## Opportunity 4 – Procedural Documentation

### Relative Priority

Low

Deploy and Communicate Strategy

Sustain Leadership

Promote Culture

Manage Community

Refresh Content and Programming

Enforce Policies and Governance

Deploy Tools

Measure and Report

### Observation

CFX's social media practices follow the Social Media policies and Social Media Procedures Manual General Guide to outline the appropriate content to be administered on social media channels, which represents a leading practice. Opportunities exist to enhance the Social Media Procedures Manual General Guide to include additional procedures.

### Recommendation

Management can consider updating Social Media Procedures Manual General Guide to include the following:

- Process of approving social media within campaigns, including any exceptions;
- The appropriate platform to utilize for a campaign to reach an intended audience and goal;
- Creation of accounts, provisioning and de-provisioning of access, account backup and recovery, and brand management for social media platforms and tools;
- Appropriate use of mobile devices to perform social media job functions;
- Social media incident response, inclusive of information leaks and brand infringements;
- Validation that recovery methods for social media accounts are available to CFX if accounts are compromised;
- Compliance with relevant laws including internal governance compliance, legal holds on social media data storage, privacy laws and data protection compliance, and public disclosures and endorsements, as applicable to CFX's environment;
- IT and Legal department involvement in the overall social media process.

### Management Response

Management concurs.

### Management Action Plan

Management will consider the recommended topics as an update to the Social Media Procedures Manual.

### Action Plan Owner / Due Date

Angela Melton, Manager of Communications and Marketing / January 31, 2021

*Face the Future with Confidence*

protiviti<sup>®</sup>

# **D.2f**

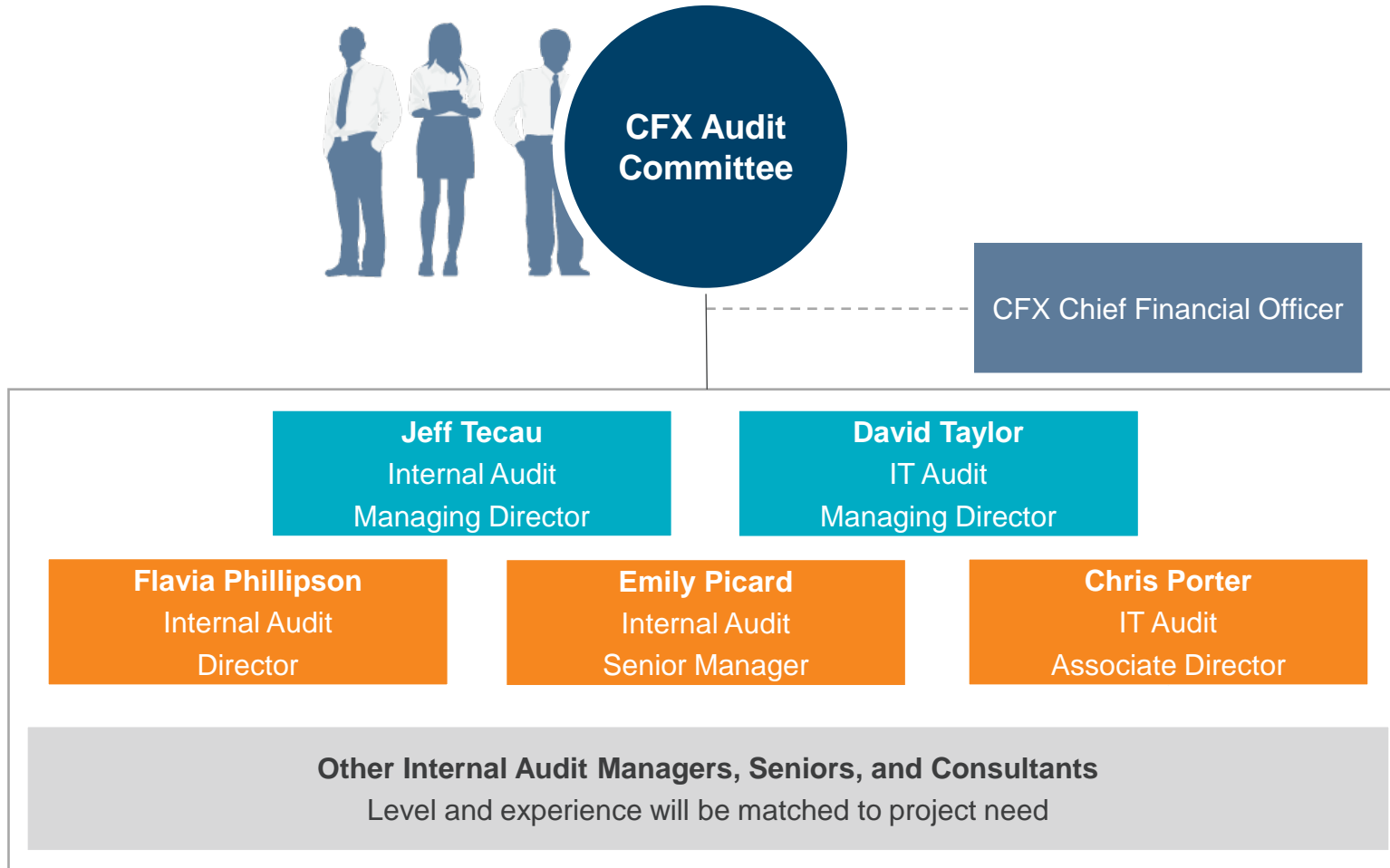
## **2021 Internal Audit Plan and Risk Assessment**

# CENTRAL FLORIDA EXPRESSWAY AUTHORITY

**Fiscal 2021 Internal Audit Plan**





For the Fiscal Year Ending June 30, 2021

# YOUR INTERNAL AUDIT TEAM



# BACKGROUND

An annual risk assessment is a critical element of a high-quality Internal Audit department’s responsibility and provides the opportunity to be “front and center” with senior leadership as a strategic partner in the review and management of key business risks. The objective of the fiscal 2021 risk assessment is to identify and prioritize key areas of risk within CFX to consider in designing the fiscal 2021 Internal Audit plan. The approach to conduct the fiscal 2021 risk assessment and develop the fiscal 2021 Internal Audit plan is depicted below.

	<h3>Identify Key Areas of Risk to be Assessed</h3>	<ul style="list-style-type: none"> <li>• Confirm and update prior year risk areas based upon review of prior year work papers, audit results, and discussions with staff</li> <li>• Determine preliminary risk ratings based upon prior year results</li> </ul>
	<h3>Assess &amp; Prioritize Areas of Risk</h3>	<ul style="list-style-type: none"> <li>• Conduct interviews with management, the Board, and the Audit Committee Chair to confirm and validate the current enterprise risk model and gain additional insight around risk trending, key changes in the organization, and key initiatives</li> <li>• Aggregate and compile resulting information</li> <li>• Provide a graphical representation of enterprise risks on a risk heat map to prioritize residual areas of risk</li> </ul>
	<h3>Select Focus Areas</h3>	<ul style="list-style-type: none"> <li>• Evaluate the prioritized enterprise risks and management commentary to determine Internal Audit focus areas for fiscal year 2021</li> <li>• Develop and define a preliminary listing of proposed Internal Audit projects to address the areas of focus</li> </ul>
	<h3>Develop &amp; Approve Audit Plan</h3>	<ul style="list-style-type: none"> <li>• Establish high-level scoping statements and levels of effort for proposed projects</li> <li>• Finalize budget allotments and propose projects for Audit Committee approval</li> <li>• Finalize proposed timing for selected projects</li> <li>• Finalize Internal Audit plan and obtain Audit Committee approval</li> </ul>



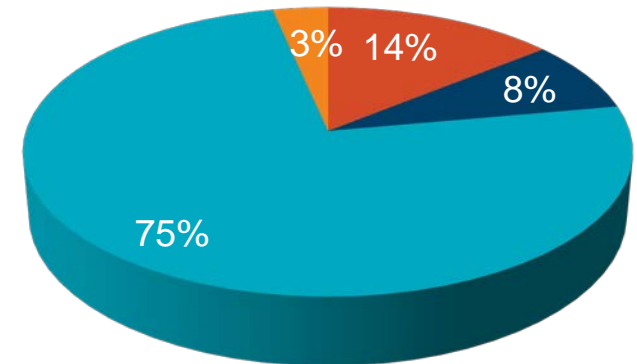
# INTERVIEW LIST

The following 14 individuals were interviewed to gather information to develop the fiscal year 2021 Internal Audit plan:

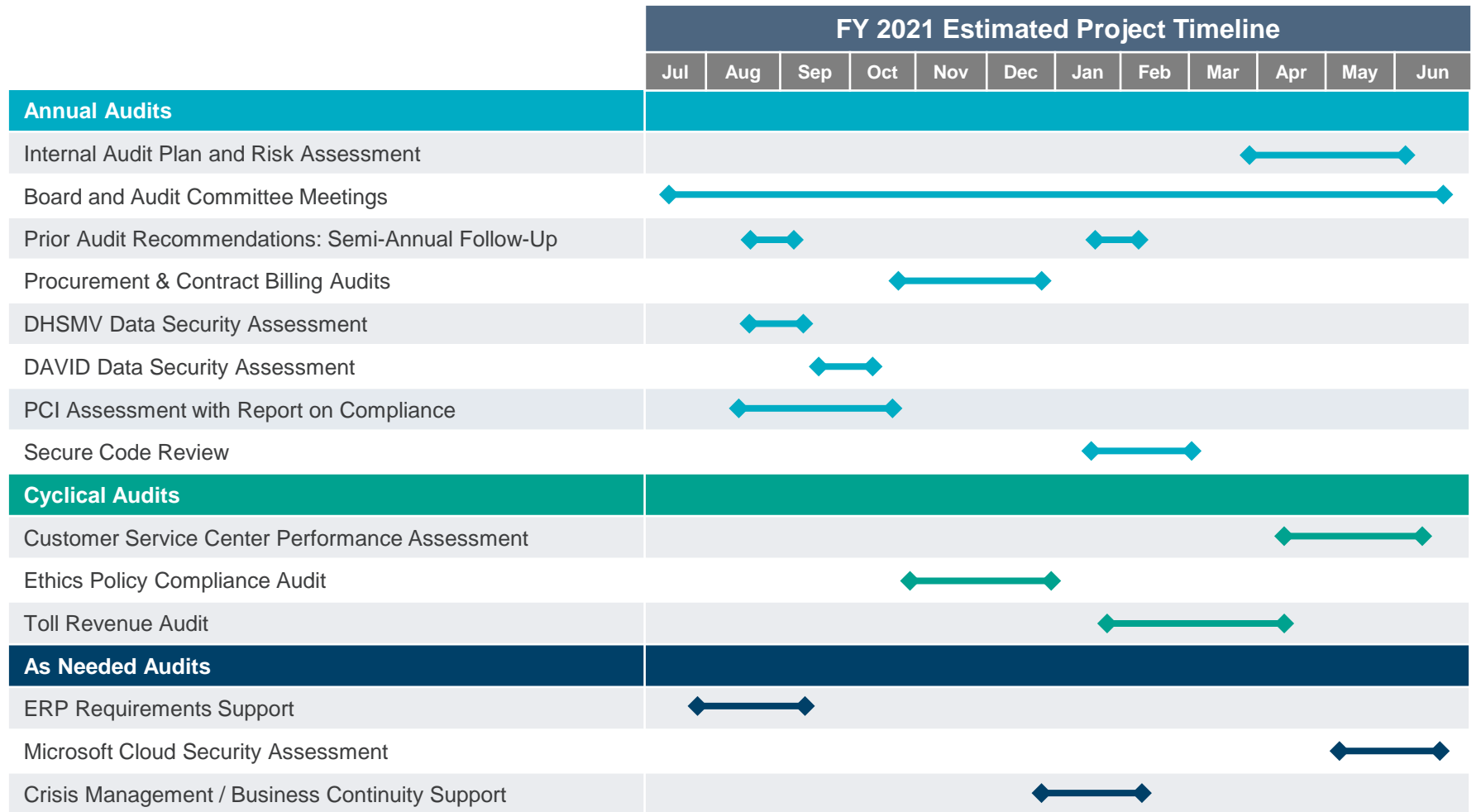
Name	Title
Kristy Mullane	Audit Committee Chair
Laura Kelley	Executive Director
Glenn Pressimone	Chief of Infrastructure
Lisa Lumbard	Chief Financial Officer
Michelle Maikisch	Chief of Staff and Public Affairs Officer
Jim Greer	Chief of Technology and Operations
Diego “Woody” Rodriguez	General Counsel
Joann Chizlett	Director of Special Projects
David Wynne	Director of Toll Operations
Evelyn Wilson	Director of Human Resources
Rafael Milan	Director of Information Technology
Michael Carlisle	Director of Accounting and Finance
Aneth Williams	Director of Procurement
Will Hawthorne	Director of Engineering

# FY 2021 INTERNAL AUDIT COVERAGE

Strategic & Governance	Budget Allocation	Frequency
<ul style="list-style-type: none"> <li>Fiscal 2022 Internal Audit Plan and Risk Assessment</li> <li>Prior Audit Recommendations: Semi-Annual Follow-up</li> <li>Ethics Policy Compliance Review</li> </ul>	\$25,000 \$15,000 \$40,000	Annual Annual 3 Year Cycle
Financial		
<ul style="list-style-type: none"> <li>Procurement &amp; Contract Billing Audits</li> </ul>	\$45,000	Annual
Operations & IT		
<ul style="list-style-type: none"> <li>DHSMV Data Security Assessment</li> <li>DAVID Data Security Assessment</li> <li>PCI Assessment with Report on Compliance</li> <li>Secure Code Review</li> <li>Toll Revenue Audit</li> <li>Microsoft Cloud Security Assessment</li> <li>Crisis Management / Business Continuity Support</li> <li>Customer Service Center Performance Assessment</li> <li>ERP Requirements Support</li> </ul>	\$25,000 \$20,000 \$85,000 \$25,000 \$80,000 \$50,000 \$40,000 \$45,000 \$50,000	Annual Annual Annual Annual 3 Year Cycle As Needed As Needed 2 Year Cycle As Needed
Other		
<ul style="list-style-type: none"> <li>Board and Audit Committee Meetings</li> <li>Contingency for Special Projects</li> </ul>	\$15,000 \$4,000	Annual Annual
<b>Total Internal Audit Budget</b>	<b>\$564,000</b>	



# INTERNAL AUDIT TIMELINE



# THREE YEAR INTERNAL AUDIT PLAN

Description	Frequency	Date Last Performed	Audit Plan Year		
			2021	2022	2023
<b>Annual Internal Audits</b>					
Internal Audit Plan and Risk Assessment	Annual	2020	X	X	X
Board and Audit Committee Meetings	Annual	2020	X	X	X
Prior Year Recommendations: Semi-Annual Follow-up	Annual	2020	X	X	X
Procurement & Contract Billing Audits	Annual	2020	X	X	X
DHSMV Data Security Assessment	Annual	2020	X	X	X
DAVID Data Security Assessment	Annual	2020	X	X	X
PCI Assessment with Report on Compliance	Annual	2020	X	X	X
Secure Code Review	Annual	2020	X	X	X
Contingency for Special Projects	Annual	N/A	X	X	X
<b>Cyclical Audits</b>					
Customer Service Center Performance Assessment	2 Year Cycle	2019	X		
Ethics Policy Compliance Audit	3 Year Cycle	2018	X		
Toll Revenue Audit	3 Year Cycle	2019	X		
IT General Controls Review	3 Year Cycle	2018		X	
Information Security Risk Assessment Refresh	3 Year Cycle	2018		X	
Bond Financing Review	5 Year Cycle	2016		X	
Right of Way Audit	5 Year Cycle	2016		X	
Business Continuity Management Review	5 Year Cycle	2017		X	
Purchasing Spend Data Audit	5 Year Cycle	2017		X	
Accounting System Access and SOD Review	5 Year Cycle	2017		X	
Human Resources Process Review	5 Year Cycle	2017		X	
Public Records and Information Management Review	3 Year Cycle	2020			X
Safety and Maintenance Policy and Procedures Compliance Audit	5 Year Cycle	2018			X
Toll Violations Audit	5 Year Cycle	2018			X
COSO ERM Governance Review	5 Year Cycle	2020			
P-Card and Gas Card Audit	5 Year Cycle	2020			
<b>As Needed Audits</b>					
ERP Requirements Support	As Needed	N/A	X		
Microsoft Cloud Security Assessment	As Needed	N/A	X		
Crisis Management / Business Continuity Support	As Needed	N/A	X		
RPA and Automation Assistance	As Needed	2020		X	
Policy and Procedure Review	As Needed	N/A		X	
Compromise Assessment	As Needed	N/A		X	
Sensitive Data Review	As Needed	2014			
ITS Security Review	As Needed	2015			
Accounting and Financial Controls Review	As Needed	2019			
IT Project Management Review	As Needed	2019			
Ransomware Review	As Needed	2019			
Cyber Security Incident Response Review	As Needed	2019			

# FY 2021 INTERNAL AUDIT PROJECT DESCRIPTIONS

#	Project	Project Description	Risks	Estimated Cost
1	<b>Internal Audit Plan and Risk Assessment</b>	We will conduct a risk assessment to highlight the Expressway Authority's current year risk profile, to identify risk trends, and to form the foundation for the fiscal year 2021 Internal Audit Plan. In addition, we will conduct the annual review of the completeness of the fraud risk universe and annual refresh of the fraud risk assessment. The information and findings will be utilized to develop the 2021 Internal Audit plan, with a focus on addressing opportunities identified during the risk assessment process.	Strategic Planning Fraud Governance	\$25,000
2	<b>Board and Audit Committee Meetings</b>	Protiviti will attend Board meetings and prepare for and present at all Audit Committee meetings during fiscal year 2021. This includes document preparation time and preparation time with management and the Audit Committee in advance of meetings.	Governance	\$15,000
3	<b>Prior Audit Recommendations: Semi-Annual Follow-up</b>	This work will focus on semi-annual follow-up on the status of all OPEN action plans from prior year audits. In addition, internal audit will consider re-auditing closed recommendations for selected areas from prior year audits as requested by management or the Audit Committee.	Governance	\$15,000
4	<b>Procurement &amp; Contract Billing Audits</b>	This audit will encompass a selection of 2 or 3 engineering, construction, maintenance, operations, or legal contracts, with the objective of verifying internal controls are in place to ensure work performed for CFX has been billed in accordance with contractual terms and conditions. The work will include reviewing procurement, reviewing contract SLA's, testing pricing and hours worked for accuracy and validity, testing invoice approvals, testing vendor compliance with other contractual obligations, and using data analytics to identify high risk vendors and/or change orders.	Contract Management Contract Performance Reporting Cost Containment Procurement and Vendor Selection	\$45,000
5	<b>DHSMV Data Security Assessment</b>	The objective of this assessment is to review internal controls for gaps in design related to the requirements set forth in the DHSMV Drivers License or Motor Vehicle Record Data Exchange Memorandum of Understanding (MOU), Section V – Safeguarding Information.	Cyber / Data Security	\$25,000

# FY 2021 INTERNAL AUDIT PROJECT DESCRIPTIONS

#	Project	Project Description	Risks	Estimated Cost
6	<b>DAVID Data Security Assessment</b>	The objective of this assessment is to review internal controls for gaps in design related to the requirements set forth in the DHSMV Driver and Vehicle Information Database ("DAVID") Data Exchange Memorandum of Understanding (MOU), Section V – Safeguarding Information	Cyber / Data Security	\$20,000
7	<b>PCI Assessment with Report on Compliance</b>	This project will be to fully test CFX's compliance with the PCI Data Security Standard, (PCI-DSS) version 3.2 and issue a Report on Compliance (ROC). The testing will cover all twelve sections of the PCI-DSS.	Cyber / Data Security	\$85,000
8	<b>Secure Code Review</b>	This review will assess the security of production code for applications that are developed in-house. Application's functionality, security standards, and coding practices will be reviewed through documentation and by conducting both automated and manual analysis against the Open Web Application Security Project ("OWASP") framework.	Cyber / Data Security	\$25,000
9	<b>Customer Service Center Performance Assessment</b>	Leveraging subject matter expertise, Protiviti will conduct an assessment of the customer contact center and consider current needs of the center, including opportunities to reduce staff turnover. The audit will involve a review of the center's performance through an organizational analysis, a customer contact analysis, an analysis of technology, infrastructure and applications, and a statistical data analysis.	Cost Containment Customer Satisfaction Public Relations	\$45,000
10	<b>Ethics Policy Compliance Review</b>	CFX has a formal ethics policy in place. Internal Audit will review the policy and (1) leverage leading practices to suggest additional areas for consideration to include in the policy and (2) review compliance with the policy, including the new provisions added as a result of Florida state legislation.	Ethical Compliance	\$40,000

# FY 2021 INTERNAL AUDIT PROJECT DESCRIPTIONS

#	Project	Project Description	Risks	Estimated Cost
11	<b>Toll Revenue Audit</b>	As CFX continues to migrate cash customers to electronic tolling and increase EPASS account conversion, a new Pay By Plate rate will be put into effect on July 1, 2020. In addition, the Infinity tolling system now generates a majority of CFX revenue with all systems “live” by the time of this audit. This audit will focus on electronic and cash tolling processes and include a review of Infinity transactions for accuracy, the Pay By Plate process and impact to collectability, and cash (manned and unmanned lanes). The audit will include review of (1) controls that verify revenue data captured at the point of origin is completely and accurately recorded to the financial statements, (2) physical safeguarding controls exist around cash (including the use of security and surveillance, data analytics, monitoring and reporting, and counts/other reconciling activities), (3) controls in place around processing revenue adjustments to customer accounts are operating according to policy, (4) changes to business processes and controls related to Pay By Plate billing, collection, and monitoring and (5) appropriate reconciliation controls are in place to monitor revenue related to interoperability agreements. Additionally, IT general controls around supporting systems and information technology will be reviewed.	Toll Collections Cash Handling IT Infrastructure / Tolling System Infrastructure Financial Reporting Statewide Interoperability National Interoperability	\$80,000
12	<b>ERP Requirements Support</b>	This project will include assisting CFX to identify ERP needs across various process owners and stakeholder groups, educating staff on potential ERP capabilities, and gathering requirements for use in the new ERP system Request For Proposal (RFP). Hours allocated to this project may also be used to provide insight into potential ERP providers and unique ERP considerations for CFX.	Financial Reporting Procurement and Vendor Selection Business / IT Application and Systems	\$50,000
13	<b>Microsoft Cloud Security Assessment</b>	Internal Audit will conduct an assessment of CFX’s Microsoft cloud computing architecture, including evaluating the strategy, capabilities, operations and processes against industry leading practices. Internal Audit will also review CFX’s strategy in determining what data is stored in the cloud as well the controls utilized to ensure that data’s integrity and availability.	Cyber / Data Security	\$50,000
14	<b>Crisis Management / Business Continuity Support</b>	This review will focus on how CFX manages Business Continuity, including IT Disaster Recovery plans and Crisis Management. The review will include an assessment of the documented plans as well as the foundational efforts that were performed to create them (such as a Business Impact Analysis). This may be adjusted into a consulting project based on the recent pandemic.	Business Continuity / Disaster Recovery	\$40,000

# APPENDIX A OTHER POTENTIAL AUDITS



# OTHER POTENTIAL AUDITS NOT SELECTED FOR FY 2021 INTERNAL AUDIT PLAN

#	Project	Project Description	Risks
1	<b>IT General Controls Review</b>	This review will focus on the Expressway Authority's Information Systems area. To accomplish this, we will assess the policies and procedures that are utilized to support the business critical applications and systems at CFX. Our approach will be to focus on the IT General Computer Controls which include the following components: Change Management, Logical Security, Physical Security, Security Administration, IT Organization & Management.	Business / IT Applications and Systems IT Infrastructure
2	<b>Information Security Risk Assessment Refresh</b>	Protiviti will conduct a risk assessment of CFX's IT function that will identify asset groupings within the environment and assign them a value so that Management may prioritize in what order to address risks posed to them. This value is based on the likelihood and potential impact of threats posed to these assets, the vulnerabilities they have, and the safeguards surrounding them. This project will be a refresh of the project conducted in FY18.	Cyber / Data Security
3	<b>Bond Financing Review</b>	CFX has \$2.8B of bonds issued and outstanding with varying terms. As part of this project, we will perform a risk assessment of the financing process, a review of the policies (including policies to procure the financial advisor, underwriter, attorneys, and others involved in the financing process), and a review of the process to structure financing deals and manage existing portfolio risk. This project may also include a review of the process to monitor bond covenant compliance.	Bond Financing / Covenant Compliance
4	<b>Right of Way Audit</b>	This audit will include a review of the processes and procedures in place to manage Right of Way land acquisitions and may include a review of legal counsel responsibilities, involvement of the ROW Committee, and internal controls around managing legal counsel and other third party costs and overall purchase price. The review may include a trending analysis of appraised cost values for recent purchases and a review of outliers.	Cost Containment Public Relations Records Management
5	<b>Purchasing Spend Data Audit</b>	This review will focus on a 100% interrogation of spending data over a three to five year history to identify opportunities for recovery such as vendor overpayments, unused vendor credits, etc. We will use proprietary tools to review the Expressway Authority's detailed spend data for areas of leakage and audit against contracts and other available information as red flags are identified. As a side benefit to any actual recoveries, we will also focus on identifying potential frauds, root causes and process improvement opportunities.	Cost Containment Fraud Procurement and Vendor Selection
6	<b>Accounting System Access and Segregation of Duties Review</b>	The financial close and related accounting processes will be reviewed for appropriate segregation of duties among CFX personnel. Protiviti-developed tools will be leveraged to verify segregation for each key accounting cycle around the following: Physical custody of assets, adjustments to accounting records, approvals of accounting transactions, and review responsibilities. In addition, we will also review access rights within the Eden financial package to verify system access restrictions appropriately support segregation of duties and to identify segregation of duties conflicts within the system. We will recommend compensating monitoring controls to the extent necessary.	Financial Reporting Fraud

# OTHER POTENTIAL AUDITS NOT SELECTED FOR FY 2021 INTERNAL AUDIT PLAN

#	Project	Project Description	Risks
7	<b>Human Resources Process Review</b>	During the Human Resource Process review, we will evaluate the Human Resource process, policies, procedures and related internal controls. The review may include recruiting and hiring; training; performance evaluations; performance, reward, and recognition; and employee terminations. The HR process and controls will be reviewed for compliance with policies and comparison to leading HR practices. Lastly, the succession planning strategy may be reviewed and compared to leading practices.	Human Resources
8	<b>Public Records and Information Management Review</b>	<p>This review will focus on CFX's records and information management processes and the four cornerstones of a sustainable information governance program:</p> <ol style="list-style-type: none"> <li>1. Compliance with internal policies and legal and regulatory requirements</li> <li>2. Operational efficiencies to minimize disruptions to business operations and improve ways to create, use and dispose of data</li> <li>3. Cost savings from practical solutions that reduce storage and retrieval costs, as well as requirements for responding to investigations, litigation or regulatory requests</li> <li>4. Defensible processes in routine business operations that allow organizations to demonstrate reasonable and good faith efforts when challenged</li> </ol> <p>Data retention surrounding electronic communications via email, mobile, and voice mail will also be reviewed to identify technology needed to assist with capturing and retaining data from such communication.</p>	Records Management
9	<b>Safety and Maintenance Policy and Procedures Compliance Audit</b>	The objective of this project will be to review the safety and maintenance policies and procedures in place, including any recent technological enhancements to safety within the system (e.g. new technology measures to help reduce the risk of wrong way driving), vendor management programs, and to test compliance with the safety and maintenance policies and procedures.	Maintenance and Safety
10	<b>Toll Violations Audit</b>	This audit will focus on reviewing the processes, policies, procedures, technology, and reporting in place around the violations process to verify the process is working as intended. Focus will be on enhancing the efficiencies around the process to review violations and to bill and collect violations revenue. Samples of deleted/voided unpaid toll notices will also be reviewed to verify there is sufficient justification for voiding.	Toll Violations Toll Collections Business / IT Applications and Systems Customer Satisfaction
11	<b>COSO ERM Governance Review</b>	This audit will involve an evaluation of the Expressway Authority's governance procedures and internal controls leveraging the COSO ERM and COSO 2013 internal control frameworks as leading practice guidelines.	Governance Ethical Compliance
12	<b>P-Card and Gas Card Audit</b>	The objective of the project will be to review P-card and Gas procurement expenditures to verify purchases are adequately supported and are for valid business purposes.	Cost Containment Fraud

# OTHER POTENTIAL AUDITS NOT SELECTED FOR FY 2021 INTERNAL AUDIT PLAN

#	Project	Project Description	Risks
13	<b>RPA and Automation Assistance</b>	This project will include assisting CFX to develop automation use cases, cost benefit analyses, and prototype bot development for an area of significant opportunity for efficiency gains.	Cost Containment
14	<b>Policy and Procedure Review</b>	CFX has experienced growth in number of people over the past few years. During this audit, Protiviti will review whether Policies and Procedures are reflective of growth. To perform the audit, Protiviti will work with CFX to inventory policies and procedures, review for periods of last update, and make suggestions to mature the process to update policies and procedures. Protiviti may also make suggestions for potential additions to policies that are selected for detailed review.	Governance
15	<b>Compromise Assessment</b>	Protiviti will conduct an assessment to determine CFX's capability to detect a compromise that has already occurred within the environment. This will include baselining activities, review of information from various tools in the environment, performing manual "hunting" activities, analyzing results, and assisting with enhancement of current capabilities.	Cyber / Data Security
16	<b>Sensitive Data Review</b>	This review will include an assessment of how sensitive data is defined and categorized, where it exists logically on the CFX network and systems, and how it is destroyed when it is no longer needed. IT will include a review of any policies that govern sensitive data (as defined by CFX). Additionally, IA will use an automated data loss prevention (DLP) scanning tool to conduct a scan on a sample of systems to confirm sensitive data is stored in appropriate network locations.	Cyber / Data Security
17	<b>ITS Security Review</b>	Protiviti will conduct an IT security review of Intelligent Transportation Systems. This review will include an assessment of access controls (physical and logical), hardening procedures, patching processes, and remote connectivity of ITS systems to identify security risks that exist in the ITS network.	Cyber / Data Security
18	<b>Accounting and Financial Controls Review</b>	The objective of this project is to conduct a current state design analysis of key processes, risks, and internal controls within the accounting function and to test the operating effectiveness of key accounting and financial reporting controls, including those designed to detect or prevent fraud. The audit will also include comparisons of CFX's accounting and financial reporting controls to leading practices.	Financial Reporting Fraud
19	<b>IT Project Management Review</b>	This project will assess CFX's ability to intake, prioritize, deliver on requests from the business. Protiviti will assess the manner in which IT requests are received and accepted, the potential risks that could impact projects, the testing procedures (including unit testing, peer review, integration, regression and user acceptance), project health metrics, change requirements, and resourcing requirements.	IT Infrastructure Business / IT Applications and Systems IT Operations Strategic Planning Communication

# OTHER POTENTIAL AUDITS NOT SELECTED FOR FY 2021 INTERNAL AUDIT PLAN

#	Project	Project Description	Risks
20	<b>Ransomware Review</b>	As part of this project, Protiviti will review CFX's ability to prevent a ransomware attack against the organization. Controls surrounding email systems, open network ports, and USB ports will be reviewed as each of these is a channel through which ransomware may enter an organization. Controls that could contain a ransomware outbreak will also be reviewed to assess the effect of an outbreak within the organization should perimeter controls fail. Backup and recovery practices will be reviewed to determine CFX's ability to resume normal business function should ransomware spread throughout the organization.	Cyber / Data Security Public Relations Insurance Coverage
21	<b>Cyber Security Incident Response Review</b>	Internal Audit will review CFX's Cyber Security Incident Response program by assessing the current incident response strategy as well as the related employee training, policies and procedures, and supporting technologies deployed throughout the environment.	Cyber / Data Security Public Relations Communication Insurance Coverage

# APPENDIX B ENTERPRISE RISK ASSESSMENT

# ENTERPRISE RISK ASSESSMENT

To assist with the development of the fiscal 2021 Internal Audit Plan, Internal Audit used the prior year risk model as the starting point for discussions with CFX management. Internal Audit asked CFX management to consider the current business environment, critical business initiatives, and prior year audit results to provide input on which risks warranted the most focus in today's environment. In addition, management was asked to identify any new risks that may not have been considered in past years for inclusion in the current risk model.

Internal Audit utilized the aggregated input obtained during interviews with CFX management and from risk surveys of management to develop a list of potential internal audit projects for fiscal 2021, with the objective being to help the Audit Committee and management mitigate areas of highest residual risk, monitor areas of high inherent risk, or to mitigate areas where risks are trending higher.

Risk is defined as follows:

## Risk:

- Is the possibility of an event occurring that will have a negative impact on the achievement of goals and objectives and could also include the cost of missing an opportunity.

## Inherent Risk:

- Is the amount of risk to the business given the environment in which it operates, without considering the application of controls. The risks identified on the following page represent the risk areas deemed most important for CFX to manage and control in order to achieve its goals and objectives.

## Residual Risk:

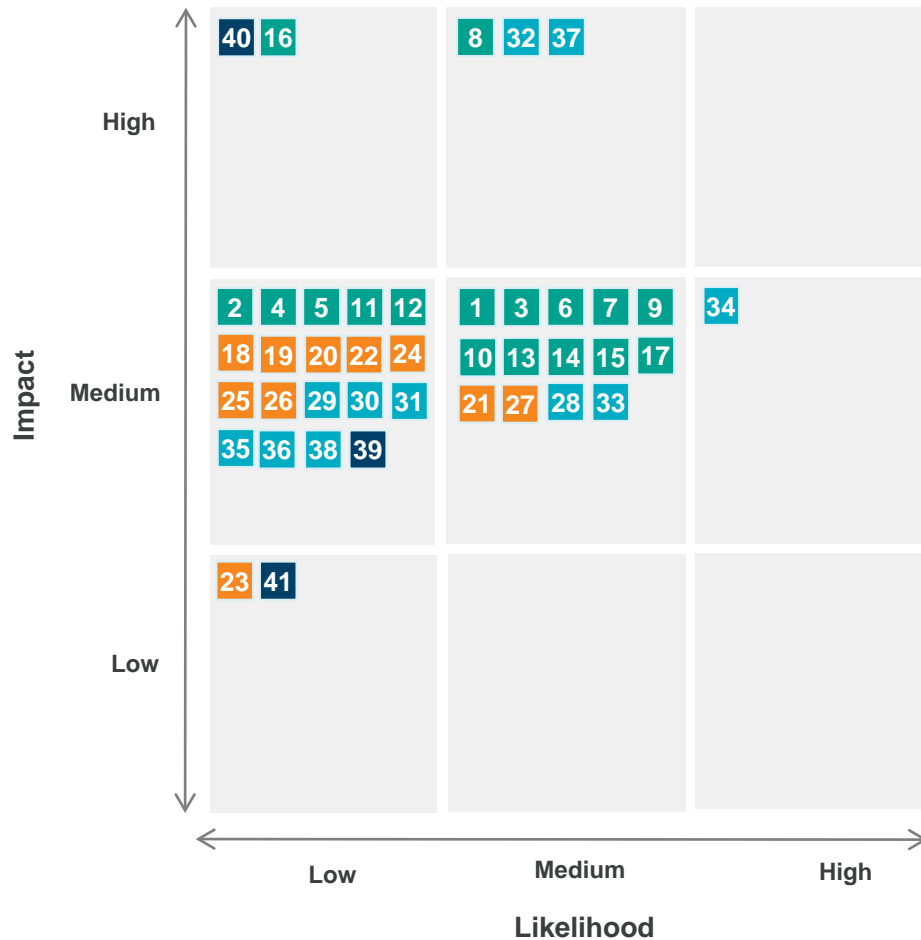
- Is the amount of risk remaining after the application of management controls. Residual risk was judgmentally considered for purposes of this fiscal 2021 audit plan in the selection of potential projects for inclusion in the plan. The results of the residual risk assessment are depicted via the Enterprise Risk Map on the following pages.

# RISK MODEL

 <b>Strategic and Governance</b>	<b>1. Strategic Planning</b>	<b>7. Governance</b>	<b>13. Public Relations</b>
	2. Organization Structure	8. Political Environment	<b>14. National Interoperability</b>
	3. Contingency Planning	<b>9. Ethical Compliance</b>	15. Toll Rate Management
	4. Regulatory Changes	10. Communication	16. Asset and Liability Transfer Risk
	5. Access to Capital	11. Leadership	17. Multimodal Opportunities
	<b>6. Statewide Interoperability</b>	12. Outsourcing	
 <b>Financial</b>	<b>18. Fraud</b>	<b>23. Cash Handling</b>	
	19. Management Performance Reporting	<b>24. Procurement and Vendor Selection</b>	
	20. Bond Financing / Covenant Compliance	<b>25. Contract Performance Reporting</b>	
	<b>21. Cost Containment</b>	<b>26. Financial Reporting</b>	
	22. Treasury and Liquidity Management	27. Right of Way	
 <b>Operations and IT</b>	28. Toll Violations	<b>34. Business Continuity / Disaster Recovery</b>	
	<b>29. Toll Collections</b>	35. Insurance Coverage	
	<b>30. Business / IT Applications and Systems</b>	<b>36. Customer Satisfaction</b>	
	31. Human Resources	<b>37. Cyber / Data Security</b>	
	<b>32. IT Infrastructure / Tolling System Infrastructure</b>	38. Toll Discounts / Rebates	
	33. IT Operations		
 <b>Regulatory and Compliance</b>	<b>39. Contract Management</b>	41. Records Management	
	40. Maintenance and Safety		

**Bold** represents risks addressed by the FY 2021 Internal Audit plan.

# 2020 ENTERPRISE RISK MAP – RESIDUAL RISK



- | Strategic and Governance |                                    | Operations and IT         |                                       |
|--------------------------|------------------------------------|---------------------------|---------------------------------------|
| 1                        | Strategic Planning                 | 28                        | Toll Violations                       |
| 2                        | Organization Structure             | 29                        | Toll Collections                      |
| 3                        | Contingency Planning               | 30                        | Business/IT Application Controls      |
| 4                        | Regulatory Changes                 | 31                        | Human Resources                       |
| 5                        | Access to Capital                  | 32                        | IT Infrastructure                     |
| 6                        | Statewide Interoperability         | 33                        | IT Operations                         |
| 7                        | Governance                         | 34                        | Business Continuity/Disaster Recovery |
| 8                        | Political Environment              | 35                        | Insurance Coverage                    |
| 9                        | Ethical Compliance                 | 36                        | Customer Satisfaction                 |
| 10                       | Communication                      | 37                        | Cyber/Data Security                   |
| 11                       | Leadership                         | 38                        | Toll Discounts/Rebates                |
| 12                       | Outsourcing                        |                           |                                       |
| 13                       | Public Relations                   | Regulatory and Compliance |                                       |
| 14                       | National Interoperability          | 39                        | Contract Management                   |
| 15                       | Toll Rate Management               | 40                        | Maintenance and Safety                |
| 16                       | Asset and Liability Transfer Risk  | 41                        | Records Management                    |
| 17                       | Multimodal Opportunities           |                           |                                       |
| Financial                |                                    |                           |                                       |
| 18                       | Fraud                              |                           |                                       |
| 19                       | Management Performance Reporting   |                           |                                       |
| 20                       | Bond Financing/Covenant Compliance |                           |                                       |
| 21                       | Cost Containment                   |                           |                                       |
| 22                       | Treasury and Liquidity Management  |                           |                                       |
| 23                       | Cash Handling                      |                           |                                       |
| 24                       | Procurement and Vendor Selection   |                           |                                       |
| 25                       | Contract Performance Reporting     |                           |                                       |
| 26                       | Financial Reporting                |                           |                                       |
| 27                       | Right of Way                       |                           |                                       |



# **D.3a**

## **Lane Scheduling and Customer Service Review**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

# **D.3b**

## **NIST Cyber Security Review – Update**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

# **D.3c**

## **Public Records and Information**

### **Management Review – Update**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

**4.**

**Annual  
Confirmation of  
No Disagreement  
with Management**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**



# **E.1**

## **Effectiveness of the Internal Control System**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

# **E.2**

## **Process for Assessing, Monitoring and Controlling Significant Risks**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

# **E.3**

**System for Monitoring  
Compliance with Laws  
and Regulations and  
Results of Investigation  
of any Instances on  
Non-Compliance**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

# **E.4**

## **Adequacy, Administration and Compliance with the Authority's Code of Ethics**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**



# **E.5**

## **Procedures for Hotline Reporting**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

**F.**

**Annual Discussion  
Regarding Internal  
Auditor  
Performance and  
Effectiveness**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

**G.**

**Annual Discussion  
Regarding Audit  
Committee and  
Individual  
Member  
Performance**

**THERE ARE NO  
BACKUP  
MATERIALS FOR  
THIS ITEM**

**H.**

**Confirmation of  
Completion of  
Responsibilities in  
the Audit  
Committee  
Charter**

# APPENDIX C

## INTERNAL AUDIT CHARTER



# INTERNAL AUDIT CHARTER

## Central Florida Expressway Authority Fiscal 2021 Internal Audit Department Charter

### Mission & Purpose

The mission of the internal audit department is to provide CFX Board with independent, objective assurance and consulting services designed to add value, improve the Expressway Authority's operations, and enhance transparency. The purpose of internal audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight into whether Expressway resources are responsibly and effectively managed to achieve intended results. The internal audit department helps the Expressway accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

### Standards & Professionalism

Internal audit will govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Definition of Internal Auditing, the Code of Ethics, and International Standards for the Professional Practice of Internal Auditing.

The Institute of Internal Auditors' Practice Advisories, Practice Guides, and Position Papers will also be adhered to as applicable to guide operations. In addition, the internal audit activity will adhere to the Expressway's relevant policies and procedures and the internal audit activity's standard operating procedures manual. Internal Audit will report periodically to senior management and the Board regarding the internal audit department's conformance to the Code of Ethics and the Standards.

### Authority

The Internal Auditor is appointed by the Expressway Authority Board, and reports to them through the Audit Committee. The role of the Internal Auditor may be filled by an outside firm that provides internal audit services to the Expressway Authority on an outsourced basis. For administrative purposes, the Internal Auditor reports to the **Chief Financial Officer**. To establish, maintain, and assure that the Expressway Authority's internal audit department has sufficient authority to fulfill its duties, the Board will:

# INTERNAL AUDIT CHARTER

## Authority (continued)

- Approve the internal audit department's charter.
- Approve the risk-based audit plan.
- Approve the internal audit department's budget and resource plan.
- Receive communications on the internal audit department's performance relative to its plan and other matters.
- Make appropriate inquiries of management and internal audit department to determine whether there is inappropriate scope or resource limitations.

Everything the Expressway Authority does is subject to assessment by internal audit. The Board authorizes the internal audit department to:

- Have full, free, and unrestricted access to all functions, records, property, and personnel pertinent to carrying out any engagement, subject to accountability for confidentiality and safeguarding of records and information.
- Allocate resources, set frequencies, select subject, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports.
- Obtain the necessary assistance of personnel in units of the organization where they perform audits, as well as other specialized service from within or outside the organization, as approved by the Audit Committee.

## Internal Audit Plan

At least annually, the Internal Audit Department will submit to senior management and the Board an internal audit plan for review and approval. The internal audit plan will consist of a work schedule as well as budget and resource requirements for the next fiscal/calendar year. The Internal Audit Department will communicate the impact of resource limitations and significant interim changes to senior management and the Board.

The internal audit plan will be developed based on a prioritization of audit universe using a risk-based methodology, including input of senior management and the Board. The Internal Audit Department will review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls. Any significant interim changes from the approved internal audit plan will be communicated to senior management and the Board through periodic activity reports.

# INTERNAL AUDIT CHARTER

## Independence & Objectivity

The internal audit activity will remain free all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If it is determined that independence or objectivity may be impaired in fact or appearance, the details of impairment will be disclosed to appropriate parties.

Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises were made, and that they do not subordinate their judgment on audit matters to others.

To ensure independence, the internal audit function has no direct responsibility or any authority over any of the activities or operations of the Expressway. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair internal auditor's judgment, including:

- Assessing specific operations for which they had responsibility within the previous year.
- Performing any operational duties for the Expressway Authority or its affiliates.
- Initiating or approving transactions external to the internal audit department.
- Directing the activities of any CFX employee not employed by the internal audit department, except to the extent that such employees have been appropriately assigned to auditing teams or to otherwise assist internal auditors.

The Internal Auditor will disclose any impairment of independence or objectivity, in fact or appearance, to appropriate parties. The Internal Auditor will exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. The Internal Auditor will make a balanced assessment of all the relevant circumstances and take necessary precautions to avoid being unduly influenced by their own interests or by others in forming judgments.

The Internal Audit Department will confirm to the Board, at least annually, the organizational independence of the internal audit activity. The Internal Audit Department will disclose to the Board any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

# INTERNAL AUDIT CHARTER

## Scope

Management is responsible for establishing and maintaining risk management, control, and governance processes. The scope of work of internal audit encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments to the Board, management, and outside parties on the adequacy and effectiveness of governance, risk management, and control processes for the Expressway Authority. Internal audit assessments include determining whether management's processes are adequate and functioning in a manner to ensure:

- Risks relating to the achievement of the Expressway Authority's strategic objectives are appropriately identified and managed.
- Interaction with the various governance groups occurs as needed.
- Significant financial, managerial, and operating information and the means used to identify, measure, analyze, classify, and report such information are relevant, reliable and understandable.
- Employee, officer, director, and contractor actions comply with policies, standards, procedures, and applicable laws, regulations, and governance standards.
- Resources and assets are acquired economically, used efficiently, and adequately protected.
- Results of programs, plans, and operations consistent with established goals and objectives are achieved.
- Operations or programs are being carried out effectively and efficiently.
- Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact the Expressway Authority.
- Quality and continuous improvement are fostered in control processes.
- Significant legislative or regulatory issues are recognized and addressed properly.
- Means of safeguarding assets are adequate and, as appropriate, existence of such assets can be verified.
- Organization's risk management processes are effective.
- Quality of performance of external auditors and the degree of coordination with internal audit are appropriate.
- Specific operations are evaluated at the request of the Board or management, as appropriate.

Internal Audit also considers relying upon the work of other internal and external assurance and consulting service providers as needed. The internal audit department may perform advisory and related client service activities, the nature and scope of which will be agreed with the Expressway Authority, provided the internal audit department does not assume management responsibility. Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during engagements. These opportunities will be communicated to the appropriate level of management.

# INTERNAL AUDIT CHARTER

## Responsibility

The internal audit department's responsibility includes, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the organization's governance, risk management, and internal controls as well as the quality of performance in carrying out assigned responsibilities to achieve the organization's stated goals and objectives. This includes:

- Ensuring each engagement of the internal audit plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.
- Ensuring the principles of integrity, objectivity, confidentiality, and competency are applied and upheld.
- Ensuring the internal audit department collectively possesses or obtain the knowledge, skills, and other competencies needed to meet the requirements of the internal audit charter.
- Ensuring trends and emerging issues that could impact the Expressway Authority are considered and communicated to senior management and the Board as appropriate.
- Ensuring emerging trends and successful practices in internal auditing are considered.
- Establishing and ensuring adherence to policies and procedures designed to guide the internal audit department.
- Ensuring adherence to the Expressway Authority's relevant policies and procedures, unless such policies and procedures conflict with the internal audit charter. Any such conflicts will be resolved or otherwise communicated to senior management and the Board.
- Ensuring conformance of the internal audit department with the Standards, with the following qualifications:
  - If the internal audit department is prohibited by law or regulation from conformance with certain parts of the Standards, the internal audit department will ensure appropriate disclosures and will ensure conformance with all other parts of the Standards.
  - If the Standards are used in conjunction with requirements issued by other authoritative bodies, the internal audit department will ensure conformance with the Standards, even if the internal audit department also conforms with the more restrictive requirements of other authoritative bodies.

# INTERNAL AUDIT CHARTER

## Reporting & Monitoring

A written report will be prepared and issued by the Internal Audit Department following the conclusion of each internal audit engagement and will be distributed as appropriate. Internal audit results will also be communicated to the Board.

The internal audit report may include management's response and corrective action taken or to be taken in regard to the specific findings and recommendations. Management's response, whether included within the original audit report or provided thereafter (i.e. within thirty days) by management of the audited area should include a timetable for anticipated completion of action to be taken and an explanation for any corrective action that will not be implemented.

The internal audit activity will be responsible for appropriate follow-up on engagement findings and recommendations, and reporting periodically to senior management and the Board any corrective actions not effectively implemented. All significant findings will remain in an open issues file until cleared.

The Internal Audit Department will periodically report to senior management and the Board on the internal audit activity's purpose, authority, and responsibility, as well as performance relative to its plan and conformance with the IIA's Code of Ethics. Reporting will also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the Board. Results of audit engagements and other activities, resource requirements, and any response to risk by management that may be unacceptable to the Expressway Authority will also be communicated periodically to the Board.

## Quality Assurance & Improvement Program

The internal audit activity will maintain a quality assurance and improvement program that covers all aspects of the internal audit activity. The program will include an evaluation of the internal audit activity's conformance with the Definition of Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

The Internal Audit Department will communicate to senior management and the Board on the internal audit activity's quality assurance and improvement program, including results of ongoing internal assessments and external assessments conducted at least every five years by a qualified, independent assessor or assessment team from outside the Expressway Authority.

# *Face the Future with Confidence*

© 2020 Protiviti Inc. All Rights Reserved. This document has been prepared for use by the CFX's 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.

protiviti®

**Central Florida Expressway**

**Audit Committee Charter Responsibilities Matrix - Fiscal Year 2020**

For Audit Committee as of June 17, 2020

**Financial Reporting Oversight**

**Review with Management and the External Auditors:**

<b>Number</b>	<b>Responsibility</b>	<b>Completion Date</b>
1a	The annual financial statement and related footnotes	<b>Oct-19</b>
1b	The external auditors' audit of the financial statements and their report	<b>Oct-19</b>
1c	Managements' representations and responsibilities for the financial statements	<b>Oct-19</b>
1d	Any significant changes required in the audit plan	<b>Oct-19</b>
1e	Information from the external auditors regarding their independence	<b>Oct-19</b>
1f	Any difficulties or disputes with Management encountered during the audit	<b>Oct-19</b>
1g	The organization's accounting principles	<b>Oct-19</b>
1h	All matters required to be communicated to the Committee under generally accepted auditing standards	<b>Oct-19</b>
2	Review with Management, the CFX's financial performance on a regular basis	<b>Oct-19</b>

**Internal Control and Risk Assessment**

3	Review with Management the effectiveness of the internal control system, including information technology security and control	<b>Jun-20</b>
4	Review with Management the effectiveness of the process for assessing significant risks or exposures and the steps Management has taken to monitor and control such risks	<b>Jun-20</b>



5	Review any significant findings and recommendations of the Internal Auditor and external auditors together with Management's responses, including the timetable for implementation of recommendations to correct any weaknesses	<b>External Auditors - Oct 19. Internal auditors - various</b>
---	---	--

**Compliance**

6	Review with Management the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up (including disciplinary action) of any instances of noncompliance	<b>Jun-20</b>
---	--	---------------

**Code of Ethics**

7	Review with Management and monitor adequacy, administration, and, compliance with the CFX's Code of Ethics	<b>Jun-20</b>
8	Review the procedures for the anonymous and confidential submission of complaints and concerns regarding matters such as accounting, internal controls, auditing, waste, abuse, fraud, conflicts of interest, or other Code of Ethics violations	<b>Jun-20</b>

**Internal Audit**

9	Recommend to the Board the appointment or removal of the Internal Audit Director	<b>As Needed</b>
10	Review and approve the annual internal audit plan and all major changes to the plan	<b>Jun-20</b>
11	Review the internal audit budget and submit to the Finance Committee	<b>Mar-20</b>
12	Review and approve the Internal Audit Department Charter	<b>Jun-20</b>
13	Review internal audit reports and recommend transmittal and acceptance of the audit for filing with the governing Board which shall be accomplished by separate item on the Consent Agenda at a regularly scheduled meeting	<b>Various</b>
14	Review annually the performance of the Internal Audit Director	<b>Jun-20</b>
15	Review annually the effectiveness of the internal audit function	<b>Jun-20</b>

**External Audit**

16	Appoint an Audit Committee Member to serve on the Selection Committee for all external audit services	<b>As Needed</b>
----	---	------------------

17	Recommend to the CFX Board the external auditors to be appointed and the related compensation	<b>Oct-19</b>
18	Review and approve the discharge of the external auditors	<b>As Needed</b>
19	Review the scope and approach of the annual audit with the external auditors	<b>Oct-19</b>
20	Approve all non-audit services provided by the external auditors	<b>As Needed</b>

**Other Authority and Responsibilities**

21	Conduct other activities as requested by the CFX Board	<b>As Needed</b>
22	Conduct or authorize investigations into any matter within the Committee's scope of responsibilities	<b>As Needed</b>
23	Address any disagreements between Management and the Internal Auditor or external auditors	<b>As Needed</b>
24	Annually evaluate the Committee's and individual member's performance	<b>Jun-20</b>
25	Review the Committee's formal Charter annually and update as needed	<b>Mar-20</b>
26	Confirm annually that all responsibilities outlined in this Charter have been carried out	<b>Jun-20</b>

**Audit Committee Composition and Chairman Selection**

27	The Audit Committee shall be composed of six voting members from Orange County, the City of Orlando, Lake County, Osceola County, Seminole County, and Brevard County and up to three (3) citizen representatives with appointment terms of 2 years.	<b>As Needed</b>
28	The Audit Committee will be chaired on an annual, rotating basis beginning on September 1, 2017 in the following order: Seminole County Representative Osceola County Representative One of Citizen Representative Lake County Representative City of Orlando Representative Brevard County Representative Orange County Representative	<b>Oct-19</b>