CENTRAL FLORIDA EXPRESSWAY AUTHORITY

AGENDA
CENTRAL FLORIDA EXPRESSWAY AUTHORITY
AUDIT COMMITTEE MEETING
March 3, 2020
10:00 AM

Meeting location: Central Florida Expressway Authority
Pelican Room #107
4974 ORL Tower Road
Orlando, FL 32807

A.   CALL TO ORDER

B.   PUBLIC COMMENT – Pursuant to Florida Statute 286.0114 the Audit Committee will allow public comment on any matter either identified on this meeting agenda as requiring action, or anticipated to come before the Committee for action in reasonable proximity to this meeting. Speakers shall be limited to three minutes per person and the assignment of one person's time to another or designation of group spokesperson shall be allowed at the discretion of the Committee Chairman.

C.   APPROVAL OF THE OCTOBER 30, 2019 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. Prior Audit Recommendations: Semi-Annual Follow-Up

   b. Procurement and Contract Billing Audit

   c. DHSMV Data Security Assessment

   d. DAVID Data Security Assessment

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

   f. Secure Code Review

E.   ANNUAL REVIEW AND APPROVAL OF THE AUDIT COMMITTEE CHARTER – Woody Rodriguez – (Action Item)

F.   INTERNAL AUDIT BUDGET FOR FISCAL YEAR 2021 – Lisa Lumbard – (Action Item)

G.   OTHER BUSINESS

H.   ADJOURNMENT

This meeting is open to the public.

Note: Any person who decides to appeal any decision made at this meeting will need record of the proceedings and for that purpose, may need to ensure that a verbatim record of the proceedings is made which includes the testimony any evidence upon which the appeal is to be based, per Florida Statute 286.0105.

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 Iranetta.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
October 30, 2019

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

Committee Members Present:
Kristy Mullane, Lake County Representative, Chairman
Brian Battles, City of Orlando Representative
Lorie Bailey Brown, Seminole County Representative
Kaye Dover, Osceola County Representative
Randy Singh, Orange County Representative
Kathy Wall, Brevard County Representative

Also Present:
Laura Kelley, Executive Director
Lisa Lumbard, Chief Financial Officer
Woody Rodriguez, General Counsel
Rita Moore, Recording Secretary/Executive Assistant
Jeff Tecau, Protiviti
Teresa Mallary, Protiviti
Chris Porter, Protiviti
David Taylor, Protiviti
Joel Knopp, MSL

A. CALL TO ORDER

The meeting was called to order at approximately 10:32 a.m. by Chairman Mullane.

Lorie Bailey Brown, Seminole County Representative and Kathy Wall, Brevard County Representative were welcomed to the Audit Committee.

All others in attendance introduced themselves.

B. PUBLIC COMMENT

There was no public comment.

C. APPROVAL OF THE JUNE 20, 2019 MINUTES

The question was raised on the procedure of voting to approve minutes if a committee member was not present at the last meeting.

This item was deferred until after the External Audit Matters were presented in order to seek General Counsel's advisement regarding the voting procedure when a committee member was not present.

D. EXTERNAL AUDIT MATTERS

1. Review and Acceptance of Audit of Fiscal 2019 Financial Statements and Required Communications

   Joel Knopp of Moore Stephens Lovelace, P.A. (MSL) presented FY 2019 Financial Statements and Single Audit Report.

   A motion was made by Ms. Mullane and seconded by Ms. Dover to review and accept the Fiscal Year 2019 Financial Statements and Fiscal Year 2019 Single Audit Report. The motion carried unanimously with six (6) members present voting AYE by voice vote.

C. APPROVAL OF THE JUNE 20, 2019 MINUTES CONT.

Mr. Rodriguez, General Counsel, arrived at approximately 10:47 a.m.

Ms. Lumbard posed the question to Mr. Rodriguez regarding the procedure of voting to approve minutes if a committee member was not present at the last meeting.

Mr. Rodriguez advised that all committee members present vote regardless of attendance at the last committee meeting.

A motion was made by Ms. Mullane and seconded by Mr. Singh to approve the June 20, 2019 minutes as presented. The motion carried unanimously with six (6) members present voting AYE by voice vote.

E. INTERNAL AUDIT MATTERS

1. Status Update: Fiscal 2020 Internal Audit Plan

    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 and budget.

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

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

    a. Fiscal 2019 IT Project Management Review

    Chris Porter of Protiviti presented the IT Project Management report and identified four important opportunities for process improvement: Framework, Intake Process, Portfolio Management, and Resource Planning.

    A discussion was had about who determines the approval of the IT projects. Mr. Greer indicated that projects above a certain dollar amount are approved at the CFX executive level

    A motion was made by Mr. Singh and seconded by Mr. Battles to accept the Fiscal 2019 IT Project Management Review report as presented. The motion carried unanimously with six (6) members present voting AYE by voice vote.

    b. Fiscal 2019 Tolling System Replacement – LENS Access Control Review

    David Taylor of Protiviti presented the Fiscal 2019 Tolling System Replacement – LENS Access Control Review with two findings regarding user access and passwords. There were no questions from the committee.

    A motion was made by Mr. Singh and seconded by Ms. Dover to accept the Fiscal 2019 Tolling System Replacement – LENS Access Control Review as presented. The motion carried unanimously with six (6) members present voting AYE by voice vote.

    c. Fiscal 2020 Prior Audit Recommendations: Semi-Annual Follow-Up

    Teresa Mallary of Protiviti presented the Fiscal 2020 Prior Audit Recommendations: Semi-Annual Follow-Up report indicating 3 past due items: 2017 Change Management Tolling System Replacement Audit, 2018 Pay by Plate Audit, and 2019 Accounting and Financials Controls Audit.

    A discussion was had about the process for revising due dates. It was determined that due dates get revised most often due to system changes.

A motion was made by Mr. Battles and seconded by Ms. Dover to accept the Fiscal 2020 Prior Audit Recommendations: Semi-Annual Follow-Up report as presented. The motion carried unanimously with six (6) members present voting AYE by voice vote.

3. Upcoming Internal Audits

    a. Fiscal 2020 Procurement and Contract Audit Selections

    Teresa Mallary of Protiviti informed the committee that two (2) contracts were identified for Audit (Egis Inc. and Transcore).

    A question was raised about the amounts of the contracts and why they were identified.

    Committee Members agreed that the indicated two contracts were appropriate.

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

F. OTHER BUSINESS

1. Legal Update: Adoption of Public Comment Procedures

Mr. Rodriguez recommended that the Committee incorporate by reference section 1-1.011 of the Rules of Procedures for Board Meetings Policy pertaining to Public Comment.

A motion was made by Ms. Mullane and seconded by Ms. Dover to approve the adoption of section 1-1.011 of the Rules of Procedures for Board Meetings Policy pertaining to Public Comment. The motion carried unanimously with six (6) members present voting AYE by voice vote.

G. ADJOURNMENT

Chairman Mullane adjourned the meeting at approximately 11:38 a.m.
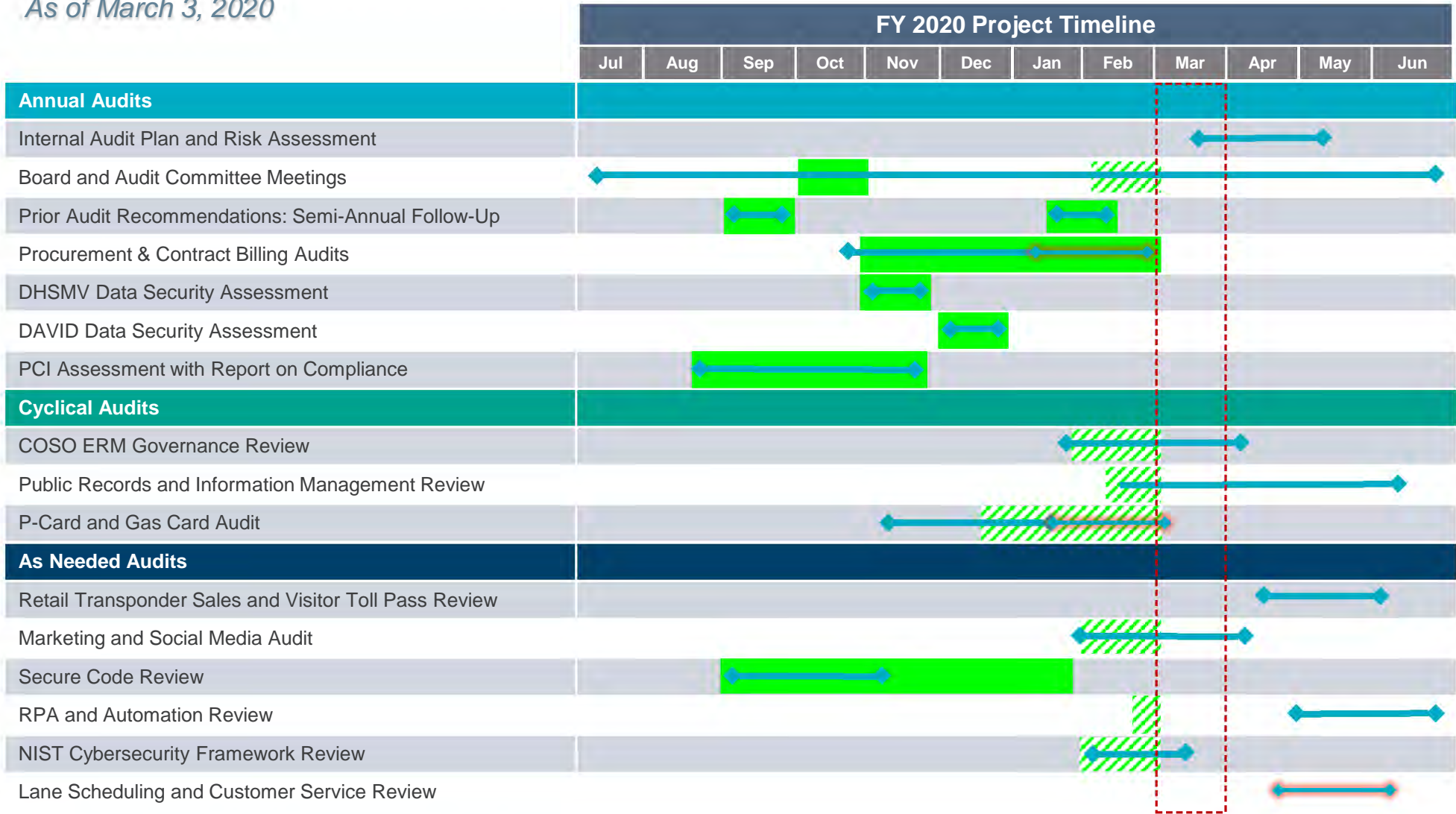
Minutes approved on _____, 2019.

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 or 4974 ORL Tower Road, Orlando, FL 32807.

D.1

3-3-20 Status Update – Fiscal 2020 Internal Audit Plan

FY 2020 Internal Audit Dashboard

As of March 3, 2020

	FY 2020 Project Timeline											
	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
Annual Audits												
Internal Audit Plan and Risk Assessment												
Board and Audit Committee Meetings												
Prior Audit Recommendations: Semi-Annual Follow-Up												
Procurement & Contract Billing Audits												
DHSMV Data Security Assessment												
DAVID Data Security Assessment												
PCI Assessment with Report on Compliance												
Cyclical Audits												
COSO ERM Governance Review												
Public Records and Information Management Review												
P-Card and Gas Card Audit												
As Needed Audits												
Retail Transponder Sales and Visitor Toll Pass Review												
Marketing and Social Media Audit												
Secure Code Review												
RPA and Automation Review												
NIST Cybersecurity Framework Review												
Lane Scheduling and Customer Service Review												

Legend: ◆—◆ Plan   ◆—◆ Revised Plan   🟢 Complete   ▨ In-Process

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

protiviti

D.2a

2020 CFX Prior Audit Recommendations Semi-Annual Follow-Up_ January

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

Prior Audit Recommendations Follow-Up

January 31, 2020

Internal Audit, Risk, Business & Technology Consulting

TABLE OF CONTENTS

protiviti

EXECUTIVE SUMMARY

Overview

As part of the Fiscal Year 2020 Internal Audit plan, Internal Audit performed a review of open audit recommendations from prior audit reports as of January 31, 2020 to verify the implementation status reported by management. Open recommendations from the following audits were evaluated:

- 2013 Toll Revenue Audit
- 2017 Change Management – Tolling System Replacement Audit
- 2018 Pay by Plate Audit
- 2018 IT General Controls Review
- 2019 Cybersecurity Incident Response

- 2019 Accounting and Financial Controls Review
- 2019 Toll Revenue Audit
- 2019 Customer Service Center Performance Review
- 2019 IT Project Management Review

Internal Audit last reviewed the status of open audit recommendations in October 2019. Results were reported to the Audit Committee at that time.

Objectives, Scope, and Approach

This review was completed as of January 31, 2020 and consisted of meetings with management to determine the status of open audit recommendations and testing of management's response and status. In addition, only those recommendations that remained open at the time of the last review have been included in this report. If a recommendation was completed as of October 15, 2019, no further work was performed, and the recommendation was not included for review.

Testing performed included inquiry with the employees responsible for completing the recommendations and/or review of documentation evidence to confirm management's reported status and explanation. In instances where the evidence obtained did not agree with management's status, discussions with management were held and the differences were resolved. There were no instances where management and Internal Audit did not come to an agreement on the status of a prior audit recommendation.

protiviti

EXECUTIVE SUMMARY

Recommendations Summary

Audit	Open as of October 15, 2019	New Action Plans	Completed as of January 31, 2020	In Progress as of January 31, 2020	Past Due
2013 Toll Revenue Audit	1	0	0	1	0
2017 Change Management - Tolling System Replacement Audit	1	0	0	1	0
2018 Pay By Plate Audit	1	0	1	0	0
2018 IT General Controls Review	1	0	0	1	0
2019 Cyber Security Incident Response Review	1	0	1	0	0
2019 Accounting and Financial Controls Audit	4	0	3	1	0
2019 Toll Revenue Audit	1	0	1	0	0
2019 Customer Service Center Performance Review	2	0	1	1	0
2019 IT Project Management Review	3	0	1	2	0
Total	**15**	**0**	**8**	**7***	**0***

* **Seven** recommendations are classified as "In Progress." **Five** of the seven recommendations are past the initial agreed-upon due date; however, these five recommendations are pending completion of a new system implementation or a procurement/vendor selection event so the due date has been revised to match the estimated timing of the necessary event. The other remaining "In Progress" recommendations are within the original, agreed-upon due date.

protiviti

STATUS OF ALL OPEN RECOMMENDATIONS

STATUS OF ALL OPEN RECOMMENDATIONS

2013 Toll Revenue Audit

Management Action Plan	Responsible Party	Status	Summary of Status	Due Date
Potential Revenue Leakage/Toll Collections Audit: CFX will automate certain aspects of the Toll Plaza Attendant's Shift Record Log by integrating tracking of unusual occurrences, violations, and insufficient fund transactions within system. This recommendation will be implemented as a function of the Tolling System replacement.	David Wynne, Director of Toll Operations	In Progress - Contingent upon Full Implementation of New Tolling System	Per discussion with Dave Wynne, Director of Toll Operations, this recommendation will be implemented within the Toll System Replacement project. The new system is currently operational except for the manned cash lanes. The implementation of this system automation includes collector buttons that are pre-designated for specific occasions and vehicles that come through the tolling lanes. Management expects the automated collector buttons to be implemented in the manned cash lanes by the revised due date of 12/31/2020.	Original: 7/1/15 Revised: 12/31/17 Revised: 12/31/19 Revised: 12/31/20

2017 Change Management - Tolling System Replacement Audit

Management Action Plan	Responsible Party	Status	Summary of Status	Due Date
TSR Vulnerability Scans: Management will remediate the Medium vulnerabilities near the completion of the TSR project.	Jim Greer, Chief of Technology and Operations	In Progress - Contingent upon Full Implementation of New Tolling System	Per discussion with Jim Greer, Chief of Technology and Operations, the remediation of these vulnerabilities is contingent upon the Toll System Replacement project completion. Management expects the Medium vulnerabilities related to the Tolling System Replacement to be completed by the revised due date of 12/31/2020.	Original: 6/30/19 Revised: 9/30/20 Revised: 12/31/20

protiviti

STATUS OF ALL OPEN RECOMMENDATIONS

2018 Pay By Plate Audit

Management Action Plan	Responsible Party	Status	Summary of Status	Due Date
Pay By Plate Program Management Procedures: The Director of Toll Operations, the Manager of E-PASS and Plaza Operations, and the Manager of VES and Special Projects will document written procedures for CFX's Pay By Plate program to address the clearly define the review and monitoring control activity. The procedures will be reviewed and updated at least annually and published on SharePoint.	David Wynne, Director of Toll Operations Paul Schatz, Manager of VES and Special Projects	Complete	Per discussion with David Wynne, Director of Toll Operations, and Paul Schatz, Manager of VES and Special Projects, Internal Audit determined that policies and procedures for the Pay By Plate program have been created and codified. Internal Audit obtained these policies and procedures and observed that review and monitoring control activities are now in place. As such, Internal Audit determined that this recommendation was implemented by the revised due date.	Original: 6/30/19 Revised: 12/31/19

protiviti

STATUS OF ALL OPEN RECOMMENDATIONS

2018 IT General Controls Review (1 – In Progress - Contingent on System Implementation) Exempt F.S.282.318

2019 Cybersecurity Incident Response Review (1 - Complete) Exempt F.S.282.318

protiviti

STATUS OF ALL OPEN RECOMMENDATIONS

2019 Accounting and Financial Controls Review

Management Action Plan	Responsible Party	Status	Summary of Status	Due Date
Vendor Master File Management: CFX will implement a review of new vendors into the Accounting Clerk's review of invoices to ensure the vendor was entered completely and accurately. CFX will further implement a review of vendor changed into the CFOs monthly review procedures.	Lisa Lumbard, CFO	In Progress - Contingent on RFP	Per discussion with the CFO, the EDEN accounting system recognizes every invoice paid as an update to the vendor within the AP module. As such, it is not possible to review monthly vendor changes as part of the current review process. The Authority is currently undergoing the RFP process to implement a new ERP system which, among other things, will allow management to review actual vendor changes in the AP module. In the meantime, the invoice review process has been updated to include a review of vendor information per EDEN against the invoice received to ensure appropriateness of the payee. The implementation of the new ERP system is expected to be completed by the revised due date of 6/30/2021.	Original: 8/31/19 Revised: 6/30/21
Year End Accounting Checklist: CFX will implement a review of the year-end accounting checklist by the Director of Accounting and Finance prior to publishing the CAFR to ensure that all procedures have been completed. The review will be evidenced through electronic sign-off on the year-end annual checklist.	Mike Carlisle, Director of Accounting	Complete	Per discussion with the Director of Accounting and Finance, and inspection of the revised checklist, Internal Audit determined that this recommendation was implemented by the prescribed due date.	Original: 12/31/19
Finalized Financial Statement Review: CFX will enhance the year end accounting checklist to include sign-off procedures for the review of the financial data with the final CAFR.	Mike Carlisle, Director of Accounting	Complete	Per discussion with the Director of Accounting and Finance, and inspection of the revised year-end checklist, Internal Audit determined that this recommendation was implemented by the prescribed due date.	Original: 12/31/19

protiviti

STATUS OF ALL OPEN RECOMMENDATIONS

2019 Accounting and Financial Controls Review (Continued)

Management Action Plan	Responsible Party	Status	Summary of Status	Due Date
Accounting Disclosure Requirements Review: CFX will implement a formalized review of the GFOA comments from the prior year's CAFR to ensure accounting and disclosure requirements are appropriately reflected in the current year CAFR. The review will be evidenced by initial on the GFOA comments by the Director of Accounting and Finance	Mike Carlisle, Director of Accounting	Complete	Per discussion with the Director of Accounting and Finance, and inspection of the revised year-end checklist, Internal Audit determined that this recommendation was implemented by the prescribed due date.	Original: 12/31/19

2019 Toll Revenue Audit

Management Action Plan	Responsible Party	Status	Summary of Status	Due Date
System Support and Maintenance: CFX will continue to monitor vendor performance and benchmark according to defined service level agreements.	Joann Chizlett, Director of Special Project	Complete	Per discussion with the Director of Special Project and inspection of the December "Monthly Performance Measures Monitoring Report" from Transcore, Internal Audit determined that this recommendation was implemented by the prescribed due date.	Original: 12/31/20

protiviti

STATUS OF ALL OPEN RECOMMENDATIONS

2019 Customer Service Center Performance Review

Management Action Plan	Responsible Party	Status	Summary of Status	Due Date
Intelligent Voice Response (IVR) Solution: CFX will develop a roadmap or strategy to update and modernize the IVR as it is integrated with the new tolling operations system.	Jim Greer, Chief of Technology and Operations David Wayne, Director of Toll Operations	In Progress - Contingent on RFP	Per discussion with the Chief of Technology and Operations, as a part of the Microsoft development for IVR, "screen pops" have been added which alert CSRs servicing customers of any data that has been already captured by the system, based on account or phone number, so that the CSR is more readily able to address the customers' needs. This process is ongoing and will be completed as part of the updates to the tolling operations system. Remediation of this finding is contingent upon an ongoing RFP; as such, the due date has been revised to 12/31/2020. The recommendation is expected to be completed by the revised due date.	Original: 12/31/19 Revised: 6/30/20 Revised: 12/31/20
Business Intelligence / Data Analytics: As CFX pursues the new tolling operations system, CFX will perform a cost analysis to evaluate the cost of capturing detailed level data for 13 months. In addition, CFX will develop a roadmap for designing dashboards and reports that contain pertinent information, performance indicators and trend analysis in a user-friendly presentation.	Jim Greer, Director of Information Technology, and David Wayne, Director of Toll Operations	Complete	Per discussion with the Chief of Technology and Operations, Internal Audit determined that a dashboard has been created within Power BI which updates in near real-time to display CMS data from a new external database. Internal Audit obtained a screenshot of the dashboard to corroborate the Chief of Technology and Operations' statements. As such, Internal Audit determined that this recommendation was implemented by the prescribed due date.	Original: 12/31/19 Revised: 12/31/20

protiviti

STATUS OF ALL OPEN RECOMMENDATIONS

2019 IT Project Management Review

Management Action Plan	Responsible Party	Status	Summary of Status	Due Date
Project Management Framework: Management will develop a plan for implementing a formalized project management framework that includes policies, procedures and templates to facilitate project management life cycles at CFX. ITIL will be considered as this framework is developed.	Jim Greer, Chief Technology and Operations Officer	In Progress	Per discussion with the Chief of Technology and Operations, remediation of this finding is in progress and expected to be completed by the original due date. No exceptions noted.	Original: 7/31/20
Resource Planning: Management will formalize resourcing practices with regard to projects at CFX based on requirements and budgets defined in the project intake process (see Observation 2). CFX will integrate these practices within the ERP system planned for 2021.	Jim Greer, Chief Technology and Operations Officer	In Progress - Contingent on RFP	Per discussion with the Chief of Technology and Operations, remediation of this finding will involve integration of CFX's timekeeping ERP system within Cherwell. As EDEN is slated to be replaced in 2021 by a new ERP system, remediation of this finding is contingent upon new ERP system implementation; the revised due date reflects this contingency. This recommendation is expected to be completed by the revised due date.	Original: 7/31/20 Revised: 6/30/21
Portfolio Management: Management will continue plans to enhance and leverage the Cherwell deployment to support the portfolio management function at CFX.	Jim Greer, Chief Technology and Operations Officer	Complete	Per discussion with the Chief of Technology and Operations and inspection of system screenshots, Internal Audit determined that remediation of this finding was completed as a part of system enhancements made within Cherwell.	Original: 3/31/20

protiviti

Face the Future with Confidence

protiviti

D.2b

CFX Procurement and Contract Billing Audit Report

PROCUREMENT AND CONTRACT BILLING AUDIT

March 2020

CENTRAL
FLORIDA
EXPRESSWAY
AUTHORITY

protiviti®
Face the Future with Confidence

Internal Audit, Risk, Business & Technology Consulting

TABLE OF CONTENTS

protiviti

EXECUTIVE SUMMARY

Overview

Overview

In accordance with the fiscal year 2020 Internal Audit Plan, Internal Audit reviewed two Central Florida Expressway Authority ("CFX") contracts with a combined contract value exceeding $145.6 million from a population of large, currently active engineering, service, maintenance, operations, and construction projects. The Procurement and Contract Billing Audit is performed by Internal Audit annually. This audit was last completed during November 2018 as part of the fiscal year 2019 Internal Audit Plan and included a different set of contracts.

Objectives

The objectives of this audit were to (1) audit the accuracy of items billed to CFX in accordance with contract terms and conditions, and (2) identify and test key processes and controls related to contract procurement, contract administration, project and cost management, and supplemental agreement management.

Project Scope and Approach

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

Phase I – Contract Analysis and Selection

To select contracts for audit, Internal Audit obtained a listing of all active contracts and identified a short-list of contracts for audit after interviewing CFX management and performing a risk analysis based on contract size, duration, terms and conditions, and nature of the work performed. The following contracts were selected for review and approved by the Audit Committee prior to audit:

1. **Egis Projects, Inc. (#001105)** – Contract for E-PASS and Violation Enforcement Operations. This contract began in August 2015 and has a current contract value of approximately $54 million. As taken from Eden, CFX's accounting system, total expenditures to date at the time of this audit were approximately $36 million. This contract was selected due to recent challenges highlighted by CFX management specific to the accuracy of invoices. This contract has not been audited previously.

2. **Transcore, Inc. (#000178)** – Contract for maintenance of toll system hardware. This contract began in July 2004 and has a current contract value of approximately $91 million. As taken from Eden, total expenditures to date at the time of this audit were approximately $80 million. This contract was selected due to the complexity of invoices and number of personnel involved in invoice review. This contract was audited in 2011.

protiviti

EXECUTIVE SUMMARY

Project Scope and Approach (Continued)

Phase II – Processes and Controls Review

Internal Audit performed audit procedures to review CFX's processes, policies, and procedures related to procurement, contract administration, project and cost management, and supplemental agreement management. Key internal controls within each of these areas were identified and tested for each contract selected in Phase I. A summary of the procedures performed, results, and observations are provided on the following pages. Additional details on the procedures performed are included in Appendix A.

In October 2019, Internal Audit completed a review of open recommendations issued as part of the prior fiscal year 2019 Procurement and Contract Billing Audit and verified that all have been incorporated into practice and policy by CFX staff. The audit recommendations issued during prior year audits were also incorporated for review as part of the Fiscal Year 2020 Procurement and Contract Billing Audit in order to verify that prior years' findings were resolved and are not prevalent in the contracts selected for testing for this audit.

Phase III – Contract-Specific Audit Procedures

Internal Audit performed detailed procedures to review contract terms, costs billed to CFX, and other key attributes for each of the contracts selected for audit. The contracts selected, value, spend to date, sample tested, and percentage of spend tested are outlined below:

Contract	Contract Value	Spend to Date [1]	Sample Tested [2]	% Spend Tested
Egis Projects, Inc.	$54,257,637	$36,260,730	$10,888,752	20%
Transcore, Inc.	$91,329,329	$80,113,029	$15,347,357	17%

[1] As of December 27, 2019

[2] Invoices were selected for testing using judgmental sampling. A detailed report of all invoices paid to date was obtained for each contract and analyzed on a month over month basis to select samples for testing. The invoices selected were tested for compliance with contract terms and conditions.

Phase IV – Reporting and Deliverables

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

protiviti

EXECUTIVE SUMMARY

Summary of Procedures and Results

For the contracts selected for audit, Internal Audit identified risks and tested key controls within the process areas outlined below. Where applicable, a sample of detailed project costs was reviewed and tested for compliance with contract terms and conditions. The table below provides an overview of the areas reviewed for each contract audited. Further details related to the specific procedures performed are provided in Appendix A.

Process	Key Areas Reviewed	Total Controls Tested	Number of Observations	Observation Reference	Relative Priority
Procurement	Project funding and bid authorization, project bidding (sealed bids and competitive sealed proposals), bid awards, bid bond requirements, and contract renewals.	18	0	-	
Contract Administration	Contract terms and conditions, insurance, bond and permitting requirements, and minority and women owned business ("MWBE") requirements.	11	0	-	
Project & Cost Management	Invoice processing, project planning, scheduling, quality control, subcontract management, cost management, owner direct material purchases ("ODMP") management, and project reporting.	13	3	1,2,3	1 – Moderate 2 – Moderate 3 – Low
Change Order Management	Supplemental agreement review, approval, and execution.	2	0	-	
Project Closeout	Preparation, approval, and submission of project close-out documents.	0	0	-	
	TOTALS:	44	3		

protiviti

DETAILED OBSERVATIONS

DETAILED OBSERVATIONS

Observation 1 – Documentation of Invoice Review

Relative Priority
Moderate

Procurement

Contract Administration

Project & Cost Management

Supplemental Agreement Management

Contract: Egis Projects, Inc. (#001105)

Observation

Through invoice testing for Egis (Contract #1105), Internal Audit identified the following instances of noncompliance with contractual terms:

- Of 20 invoices tested, two invoices contained charges related to mobilization for which no detailed supporting documentation was provided. Further, no documentation was retained by the reviewer to evidence that the missing support was investigated.
  - Note: The two invoices identified were dated prior to Supplemental Agreement #4 in June 2018.

- Of 20 invoices tested, 14 invoices contained expenses attributable to subcontractors. For 10 of the invoices with subcontractor amounts, no supporting documentation was provided, and no documentation was retained to evidence that the missing support was investigated.
  - Note: The 10 invoices identified were dated prior to process and control changes implemented in February 2019.

- Of 20 invoices tested, six invoices contained timecards for employees incurring overtime, which was not in accordance with the contract terms at the time. Additionally, the invoice review was not adequately documented to evidence that the reviewer detected and obtained approval for the payment of overtime.
  - Note: The six invoices identified were dated prior to process and control changes implemented in early 2018.

Additionally, no contract compliance checklist exists for either of the two contracts reviewed. Contract compliance checklists are employed as leading practice to ensure invoices are reviewed to a sufficient degree of precision, to ensure invoices accord with any relevant provisions of the related contract, and to document exceptions to those provisions. Without clear documentation of specific contractual provisions, invoice reviews may not be adequate to detect errors and instances of noncompliance with contractual terms.

protiviti

DETAILED OBSERVATIONS

Observation 1 – Documentation of Invoice Review

Relative Priority

Moderate

Procurement

Contract Administration

Project & Cost Management

Supplemental Agreement Management

Contract: Egis Projects, Inc. (#001105)

Recommendation

Management should implement and document a formal contract compliance checklist for the contracts selected that identifies key contract terms and CFX billing policies. The Contract Support Specialist performing the detailed invoice review should utilize the checklist to ensure all key billing contract terms and CFX billing policies are met for each invoice. Due to the complexity of the contracts selected and invoice review process, CFX should utilize the contract compliance checklist to document the review process, notes, and other pertinent information.

Management Response

Management concurs.

In relation to the departures identified, CFX made the following process changes prior to the audit:
- As of June 2018, CFX signed Supplemental Agreement #4 discontinuing further mobilization fees.
- As of February 2019, CFX began requesting company-level detail from the vendor to identify and monitor subcontractor employees.
- As of early 2018, CFX began retaining formal documentation of overtime amounts identified on the invoices and any relevant corrections.

Management Action Plan

CFX will ensure the Contract Support Specialist utilizes a contract compliance checklist to document the review of contractor invoices. CFX will leverage the contract compliance checklists already developed in the construction and engineering departments as a template. Additionally, CFX will ensure that detailed documentation is retained for any invoices approved despite containing instances of noncompliance per the checklist (detailed notes, email attachments, etc.).

Management Action Plan

Claritza Yeagins, Contract Support Specialist, 6/30/2020

protiviti

DETAILED OBSERVATIONS

Observation 2 – Contract Terms and Dispute Resolution

Relative Priority
Moderate

Procurement

Contract Administration

Project & Cost Management

Supplemental Agreement Management

Contract: Egis Projects, Inc. (#001105)

Observation

Through invoice testing, Internal Audit identified ambiguity around key contract terms related to Method of Compensation, Mobilization & Transition Plan, and Reporting for Subcontractors. In these areas, invoiced amounts that did not comply with contract terms appeared to be approved by CFX management via other means (email, task order, etc.). However, approvals for these departures from the contract were not documented timely in all cases and no formal process exists for consistently documenting and resolving contractual language and interpreting disputes with the vendor.

Recommendation

Management should review the contract terms identified during the audit for opportunities to increase clarity in subsequent contracts for this service. Management should also establish an internal procedure for documenting vendor disputes and assigning decision-making authority to appropriate representatives within the department and the executive team for resolution of disputes.

Management Response

Management concurs.

Management Action Plan

CFX will review selected contract terms to identify areas for increased clarity in future contracts. Additionally, CFX will implement an internal procedure to guide the documentation and resolution of disputes with vendors by designating responsible independent parties on the Executive Team and/or Legal to act as the final decision-making authority in contractual disputes.

Action Plan Owner / Due Date

Lisa Lumbard, CFO, 6/30/2020

protiviti

DETAILED OBSERVATIONS

Observation 3 – Invoice Review and Vendor Monitoring

Relative Priority

Low

Procurement

Contract Administration

Project & Cost Management

Supplemental Agreement Management

Contract: Egis Projects, Inc. (#001105)

Observation

Utilization of subcontractors is tracked via the EDEN financial reporting system and periodically monitored to measure compliance with any relevant contractual provisions. As invoices are processed, any amounts attributable to subcontractors are manually entered into EDEN by the Finance Department and are reflected in the EDEN Subcontract Report.

One Egis invoice selected for testing contained $12K of charges for a subcontractor which was not reflected in the Subcontract Report for the vendor. In addition, Internal Audit was unable to confirm that the EDEN Subcontract Report for this contract completely and accurately captured all subcontractor spend.

A lack of reliable subcontractor data within EDEN could impair the Authority's ability to enforce approval requirements under the procurement policy and monitor vendor compliance with contractual provisions regarding utilization of Minority Business Enterprises ("MBEs") and Women's Business Enterprises ("WBEs").

Recommendation

Management should implement and document a formal review to ensure any expenses attributable to subcontracts are accurately captured within EDEN for each invoice processed.

Management Response

Management concurs.

Management Action Plan

CFX has implemented a reconciliation of expenses allocated to subcontractors in each invoice against EDEN as part of the invoice review performed by the Manager, Contract Compliance, and will begin evidencing review through signature on the billing checklist (upon implementation). Additionally, the Supervisor of Quality Control--Toll Operations, is performing a historical audit of all subcontractor-related expenses for the selected contract and will update EDEN data upon completion.

Action Plan Owner / Due Date

Carrie Baker, Manager of Contract Compliance, 6/30/2020

protiviti

APPENDIX A

Detailed Audit Procedures Performed

APPENDIX A
Detailed Audit Procedures Performed

Procurement

Internal Audit performed detailed audit procedures related to the procurement, bidding, award, and renewal of all contracts selected for testing. The procedures performed included:

- ❖ High level review of the process for establishing bid estimates for large construction contracts;

- ❖ Testing of Board approval to advertise for bids and proposals and Board approval of the contract award;

- ❖ Testing for the use of five-year contract terms and the option for five one-year renewals for contracts;

- ❖ Testing of the key components of the competitive sealed bid and proposal processes, including:

  - Completion and utilization of bidding and award schedules;

  - Timestamps applied to all received proposals and compliance with submission deadlines;

  - The use of bid opening and bid tabulation sheets;

  - Performance of unbalanced bid reviews for competitive bids;

  - Completion of disclosure forms by CFX's employees responsible for evaluating technical and price proposals; and

  - Comparison of evaluation and scoring to advertised request for proposals.

- ❖ Completion and distribution of the monthly expiring contracts report by the procurement department; and

- ❖ Completion and approval of the expiring contract renewal worksheet and Board approval of contract renewals.

protiviti

APPENDIX A

Detailed Audit Procedures Performed

Contract Administration

Internal Audit performed detailed audit procedures related to key contract terms and conditions utilized by CFX including the satisfaction of insurance, bonding, permitting and MWBE requirements by the contractors selected for testing. The procedures performed included:

- ❖ Testing for the review of contracts by CFX's Legal Counsel;

- ❖ Testing of key contract reviews and clauses, including:

    - ▪ Right to review by CFX's Legal Counsel; and

    - ▪ Inclusion of key right to audit, termination, and indemnity clauses.

- ❖ Outlining and testing of insurance, bonding, and permitting requirements specific to the contracts selected; and

- ❖ Satisfaction of MWBE requirements set forth in the original bid and as required by CFX.

Change Order Management

Internal Audit performed detailed audit procedures related to supplemental agreement execution, review, and approval. The procedures performed included:

- ❖ Testing for Board approval of all supplemental agreements in excess of $50,000;

- ❖ Testing for the approval of all supplemental agreements by the appropriate parties;

- ❖ Testing of adequate supporting documentation for compliance with contract terms and conditions regarding price and scope for all executed supplemental agreements related to the construction contracts selected for review; and

- ❖ Testing of a sample of fuel price and bituminous mix adjustments related to the construction contracts selected for review.

protiviti

APPENDIX A

Detailed Audit Procedures Performed

Project & Cost Management

Internal Audit performed detailed audit procedures related to invoice processing and approval, project planning, scheduling and quality control, project cost management and reporting, subcontractor management, CEI oversight, and ODMP processing, where applicable based on the contract type and terms. The procedures performed included:

❖ Testing of a sample of invoices for the projects selected for adequate review and approval by the appropriate personnel and compliance with CFX's invoice processing procedures;

❖ Discussion of current practices regarding quality control, risk management plans and performance, and quality monitoring;

❖ Testing of subcontractor approval and a sample of payments made to subcontractors;

❖ Detailed testing of costs billed for a sample of invoices selected for each of the service contracts selected, and detailed testing of a sample of the quantities billed for each of the construction contracts selected;

❖ Utilization and monitoring of the CEI Consultants assigned to construction contracts;

❖ Discussion and limited testing of changes to project schedules;

❖ Review of reporting submitted to management on a regular basis; and

❖ Detailed testing of the ODMP programs implemented for the construction contracts selected.

Project Close-Out

Internal Audit performed detailed audit procedures related to completion of payments, Document Summary Manual from the CEI, and the contract closeout checklist. The procedures performed included:

❖ Testing of the completion of key project closeout documents; including submission of final payment, completion of the Document Summary Manual by the CEI, and completion of the contract closeout checklist with supporting documentation.

protiviti

Face the Future with Confidence

protiviti®

D.2c

2020 CFX DHSMV Data Security Audit Report – 1-23-2020

DHSMV Data Security Assessment

Central Florida Expressway Authority

January 2020

Table of Contents

Executive Summary

Overview

During the period of December 9, 2019 to December 20, 2019, Internal Audit performed a Data Security Assessment of the Department of Highway Safety and Motor Vehicles ("DHSMV") data within the Central Florida Expressway Authority ("CFX") environment. The objectives of the assessment were to review internal controls for gaps in design related to the requirements set forth in *Section V – Safeguarding Information*, of the DHSMV Drivers License or Motor Vehicle Record Data Exchange Memorandum of Understanding ("MOU").

The summarized objectives of Section V are:

- Information exchanged will not be used for any purposes not specifically authorized by the MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purposes, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.

- Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.

- Access to the information will be protected in such a way that unauthorized persons cannot review or retrieve the information.

- All personnel with access to the information exchanged under the terms of the MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party (CFX).

- All personnel with access to the information will be instructed of, and acknowledge their understanding of, the criminal sanctions specified in state law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party (CFX).

- All access to the information must be monitored on an on-going basis by the Requesting Party (CFX). In addition, the Requesting Party (CFX) must complete an annual audit to ensure proper and authorized use and dissemination.

Scope and Approach

Internal Audit conducted an assessment of the process used for safeguarding DHSMV data in the CFX environment. In order to complete this review, the following procedures were performed:

- Reviewed policies and procedures related to the safeguarding of electronic and physical data transfers, data storage, and data access.

- Conducted interviews with key personnel to understand the *Drivers License or Motor Vehicle Record Data Exchange* process.

- CFX Management approved the scope of work and believed it to be sufficient to meet the requirements of the MOU. Conducted testing of controls related to the following areas:

  - Policies and Procedures
  - Application Access
  - Segregation of Duties
  - Change Control
  - Data Storage
  - Data Transfer
  - Network Firewall
  - Network Architecture
  - Active Directory
  - Physical Security

- After testing was completed, analysis was performed to compare the results of testing to the control objectives outlined in the MOU.

Summary of Results

As a result of this review, Internal Audit identified zero (0) observations that should be addressed in order to enhance CFX's Drivers License or Motor Vehicle Data Exchange process.

Appendix A – Controls Tested

	Control Objective	Control Description	Testing Results
1	Information exchanged will not be used for any purposes not specifically authorized by this agreement. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.	**Policies and Procedures:** CFX implements company-wide policies and procedures that enforce the safeguarding of company data and other sensitive customer data whether or not it is currently being used or accessed.	**Control Effective**
2	All personnel with access to the information exchanged under the terms of the Drivers License or Motor Vehicle Record Data Exchange MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the requesting party.	**Training:** CFX requires in the hiring process that all users sign an acknowledgement after reviewing either the employee or contractor security guidelines handbook which covers the safeguarding of data. These acknowledgments must be maintained for all current/active users.	**Control Effective**
3	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**TRIMS Access:** System access to the TRIMS applications for new users is appropriately administered through the submission of a New User Authorization Form. This form is completed by the new user's Manager and the proper approvals/signatures are obtained. Access to the applications is then administered by IT support.	**Control Effective**
4	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**TRIMS Access - Terminated Users:** System access to the TRIMS application and company network is appropriately revoked in a timely fashion for terminated users. Upon receipt of a termination notification (email, authorization form, phone call, etc.) from HR or a Manager responsible for the terminated user, the user's system account is disabled immediately.	**Control Effective**

protiviti ®
Face the Future with Confidence

	Control Objective	Control Description	Testing Results
5	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Database-level Access:** Database-level access is restricted to the appropriate individuals through the use of unique accounts.	**Control Effective**
6	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Server-level Access:** Server-level access is restricted to the appropriate individuals through the use of unique accounts.	**Control Effective**
7	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**FTP Gateway Access:** All individuals / user accounts with access to the FTP Gateway are authorized and appropriate.	**Control Effective**
8	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Host (HT250) Access:** All individuals / user accounts with access to the Host (HT250) are authorized and appropriate.	**Control Effective**
9	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Oracle DB Access:** All individuals / user accounts with access to the Oracle DB are authorized and appropriate.	**Control Effective**
10	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**DOCPRD2 Access:** All individuals / user accounts with access to the DOCPRD2 server are authorized and appropriate.	**Control Effective**
11	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Infoview Crystal Reports (RPTPRD4) Server Access:** All individuals / user accounts with access to the Infoview Crystal Reports (RPTPRD4) server are authorized and appropriate.	**Control Effective**
12	Information exchanged will not be used for any purposes not specifically authorized by this agreement. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.	**DHSMV Data Access:** Management performs a periodic review of user access across each of the in-scope entities to ensure that the assigned access level is commensurate with his/her job function.	**Control Effective**

	Control Objective	Control Description	Testing Results
13	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Change Control / Patch Management:** Dedicated test environments exist for the testing of changes and patches, where practical. CFX appropriately documents and tests each change.	**Control Effective**
14	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Change Control / Patch Management:** All changes and patches are authorized, executed, and documented according to stated procedures.	**Control Effective**
15	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Data Encryption:** Driver's license number as it is obtained from the DHSMV is encrypted when stored in the Oracle database.	**Control Effective**
16	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Network - Firewall:** CFX has an operational firewall in place to restrict access to the internal network.	**Control Effective**
17	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Network - Active Directory:** All individuals with Active Directory credentials are current, active users and all rights granted through Active Directory are commensurate with their current job responsibilities.	**Control Effective**
18	Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.	**Physical Security - Data Center:** Access to the data center(s) is restricted to appropriate personnel and is provided through the use of a physical key or key card.	**Control Effective**
19	Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.	**Physical Security - Work Areas:** Access to the work areas is restricted to appropriate personnel and is provided through the use of a physical key or key card.	**Control Effective**

	Control Objective	Control Description	Testing Results
20	All access to the information must be monitored on an on-going basis by the Requesting Party. In addition the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination.	**Logging & Monitoring:** Logging and auditing functions are enabled on all in-scope entities. In addition, all system logs are monitored for unauthorized access and irregular activity.	**Control Effective**
21	All access to the information must be monitored on an on-going basis by the Requesting Party. In addition the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination.	**Vulnerability Scanning / Penetration Testing:** CFX performs periodic external vulnerability scans and penetration tests.	**Control Effective**

D.2d

2020 CFX DAVID Data Security Audit Report – 1-23-2020

DAVID Data Security Assessment

Central Florida Expressway Authority

January 2020

Table of Contents

Executive Summary

Overview

During the period of December 9, 2019 to January 17, 2020, Internal Audit performed a Data Security Assessment of the Driver and Vehicle Information Database systems ("DAVID") data within the Central Florida Expressway Authority ("CFX") environment. The objectives of the assessment were to review internal controls for gaps in design related to the requirements set forth in *Section V – Safeguarding Information*, of the DHSMV Driver and Vehicle Information Database Data Exchange Memorandum of Understanding ("MOU").

The summarized objectives of *Section V* are:

- Information exchanged will not be used for any purposes not specifically authorized by the MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purposes, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.

- The Requesting Party shall not indemnify and shall not be liable to the Providing Agency for any driver license or motor vehicle information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to the MOU, except as otherwise provided in Section 768.28, Florida Statutes.

- Any and all DAVID-related information provided to the Requesting Party (CFX) as a result of the MOU, particularly data from the DAVID system, will be stored in a place physically secure from access by unauthorized persons.

- The Requesting Party shall comply with Rule 74-2, Florida Administrative Code, and with Providing Agency's security policies, and employ adequate security measures to protect Providing Agency's information, applications, data, resources, and services.   The applicable Providing Agency's security policies shall be made available to Requesting Party.

- When printed information from DAVID is no longer needed, it shall be destroyed by cross-cut shredding or incineration.

- The Requesting Party (CFX) shall maintain a list of all persons authorized within the agency to access DAVID information, which must be provided to the providing agency upon request.

- Access to DAVID-related information, particularly data from the DAVID System, will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.

- Under the MOU agreement, access to DAVID shall be provided to users who are direct employees of the Requesting Party (CFX) and shall not be provided to any non-employee or contractors of the Requesting Party (CFX).

Scope and Approach

Internal Audit conducted an assessment of the process used for safeguarding DAVID data in the CFX environment. In order to complete this review, the following procedures were performed:

- Reviewed policies and procedures related to the safeguarding of electronic and physical data transfers, data storage, and data access.

- Conducted interviews with key personnel to understand the *Drivers and Vehicle Information Database System Data Exchange* process.

- CFX Management approved the scope of work and believed it to be sufficient to meet the requirements of the MOU. Performed testing of controls related to the following areas:

  o Policies and Procedures
  o Application Access
  o Risk Management
  o Change Control
  o Data Storage
  o Data Transfer
  o Network Firewall
  o Network Architecture
  o System Authentication
  o Access Controls
  o Physical Security

- After testing was completed, analysis was performed to compare the results of testing to the control objectives outlined in the MOU.

Summary of Results

As a result of this review, Internal Audit identified zero (0) observations that should be addressed in order to enhance CFX's Driver and Motor Vehicle Database system Data Exchange process.

Appendix A – Controls Tested

	Control Objective	Control Description	Testing Results
1	Document and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations.	**Policies and Procedures:** CFX has identified cybersecurity legal and regulatory requirements and identified individuals responsible for managing requirements.	**Control Effective**
2	Ensure governance and risk management processes address cybersecurity risks.	**Risk Management:** CFX has documented risk management processes in place to address cybersecurity risks.	**Control Effective**
3	Identify and prioritize risk responses, implement risk mitigation plans, and monitor and document plan implementation.	**Risk Management:** CFX has implemented risk management processes in place to mitigate risks identified.	**Control Effective**
4	Determine risk tolerance as necessary, based upon: their analysis of sector specific risks; the agency's industry sector; agency-specific risks (e.g., Health Information Portability Accountability Act of 1996 compliance for agencies that maintain this information); and the agency's role in the state's mission.	**Risk Management:** CFX has implemented risk management processes in place to identify industry specific risks.	**Control Effective**
5	Establish parameters for IT Staff participation in procurement activities.	**Procurement Activities:** CFX has implemented policies and procedures for procurement activities.	**Control Effective**
6	Identify the IT issues IT staff must address during procurement activities (e.g., system hardening, logging, performance, service availability, incident notification, and recovery expectations).	**Procurement Activities:** CFX has implemented policies and procedures to ensure proper requirements are addressed during procurement activities.	**Control Effective**

protiviti ®
Face the Future with Confidence

	Control Objective	Control Description	Testing Results
7	Prior to introducing new IT resources or modifying current IT resources, perform an impact analysis. The purpose of this analysis is to assess the effects of the technology or modifications on the existing environment.	**Change Control:** Changes are classified prior to implementation to identify the effects of changes within the environment. CFX appropriately documents and tests each change.	**Control Effective**
8	Ensure that privileged users understand their roles and responsibilities.	**Privileged Access:** All individuals / users with privileged access are aware of their responsibilities to CFX's data security.	**Control Effective**
9	Maintain adequate capacity to ensure system availability and data integrity.	**System Monitoring:** CFX has implemented automated mechanisms to monitor system capacity and data integrity.	**Control Effective**
10	Integrity checking mechanisms are used to verify hardware integrity.	**Hardware Integrity:** Access to physical devices is restricted to authorized individuals and additional integrity monitoring is in place to detect changes to critical system files associated with hardware devices.	**Control Effective**
11	Ensure backups of information are conducted, maintained, and tested periodically.	**Backup Procedures:** Backups are conducted and tested periodically.	**Control Effective**
12	Establish a policy and procedure review process that facilitates continuous improvement to protection processes.	**Security Improvement:** CFX has implemented a risk assessment process to monitor and facilitate improvement of security controls currently in place.	**Control Effective**
13	Ensure that effectiveness of protection technologies is shared with stakeholders that should or must receive this information.	**Technology Effectiveness:** CFX communicates the effectiveness of implemented technologies related to cybersecurity when deemed necessary.	**Control Effective**
14	Each agency shall perform maintenance and repairs of information systems and components consistent with agency-developed policies and procedures.	**System Maintenance:** Maintenance on in-scope systems is documented and performed by appropriate personnel or approved vendors where maintenance agreements are in place.	**Control Effective**

	Control Objective	Control Description	Testing Results
15	Not engage in new development of custom authenticators. Agencies assess the feasibility of replacing agency-developed authenticators in legacy applications.	**Authentication Mechanisms:** CFX utilizes Active Directory authentication on in-scope systems. For systems not utilizing Active Directory authentication, CFX utilizes .NET authentication frameworks for one in-scope system with plans to implement Active Directory authentication for future system implementation.	**Control Effective**
16	Protect and restrict removable media in accordance with agency-developed information security policy.	**Removable Media:** CFX has implemented controls to prevent removable media where not required for business purposes.	**Control Effective**
17	Protect communications and control networks by establishing perimeter security measures to prevent unauthorized connections to agency IT resources.	**Network Firewall:** CFX has an operational firewall in place to restrict access to the internal network.	**Control Effective**
18	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**System Availability:** CFX has implemented a redundant data center to provide resiliency in the event of system outages.	**Control Effective**
19	Each agency shall develop policies and procedures that will facilitate detection of anomalous activity in a timely manner and that will allow the agency to understand the potential impact of events. Such policies and procedures shall establish and manage a baseline of network operations and expected data flows for users and systems	**Logging & Monitoring:** Logging and auditing functions are enabled on all in-scope entities. In addition, all system logs are monitored for unauthorized access and irregular activity.	**Control Effective**
20	Monitoring for unauthorized personnel, connections, devices, and software.	**Access Controls:** CFX has implemented badge access and cameras at facilities, and firewalls, file integrity, and antivirus software on systems to restrict access to the internal network, and unauthorized software.	**Control Effective**

protiviti ®
Face the Future with Confidence

D.2e

CFX 2019 PCI Assessment with Report on Compliance

PCI Data Security Standard

The assessment focused on over 400 controls within the following twelve domains of the PCI Data Security Standard

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

protiviti®

Summary of the Assessment

- Protiviti team performed onsite and remote fieldwork between July 11, 2020 through October 26, 2020.

- Fieldwork was conducted through a variety of methods including documentation review, interviews, technical analysis, and physical investigation.

- All CFX individuals involved were extremely helpful and well attuned to the importance of the assessment.

protiviti®

Face the Future with Confidence

D.2f

CFX Secure Code Review Report - Summary

CENTRAL FLORIDA EXPRESSWAY AUTHORITY SOURCE CODE REVIEW - SUMMARY

2/23/2020

Table of Content

Internal Audit, Risk, Business & Technology Consulting

I. Executive Summary

Background

In Q3 2019, CFX engaged a third party, Protiviti, to perform web application and secure code review of five (5) applications. The project focused on evaluating controls that directly correlate to threats and risks that may compromise the confidentiality, integrity, and availability of systems or proprietary information that reside on CFX infrastructure.

Fieldwork was performed remotely from Protiviti security labs in Philadelphia, PA between August 19, 2019 and September 13, 2019. Protiviti performed retesting of several vulnerabilities as requested by CFX to confirm successful remediation during the engagement.

Objectives and Scope

This engagement was executed with the intent of assessing existing controls within the web application that are designed to minimize the risks to the organization. As such, Protiviti attempted to identify security vulnerabilities, circumvent security controls, and to execute authorized exploits within the application. Emphasis was placed on evaluating application controls that restrict unauthorized access to the CFX applications, the data it transmits, and the critical account data (e.g. credentials, PHI data, etc.) it stores.

The scope of the security assessment included the following:

- **Web Application Security Testing (EpassWeb**) – Performed a series of security tests against the web application using automated commercial application scanning tools and web application proxies to crawl and map the target applications. Specifically, application entry points, programming languages, structure, and error codes were identified to complete the application mapping process. Protiviti leveraged the data collected from the crawling and mapping phase to perform a series of automated tests, manual tests, and validation activities to evaluate the security posture of the application.

- **Secure Source Code Review (Epass Mobile, Web API, Epass Web, VesWeb)** – Performed source code analysis using automated static code analysis tools to find potential issues within the web application source code. Protiviti then performed manual false positive analysis to validate identified vulnerabilities. Manual analysis was then performed to identify issues that were not identified during the automated process.

 Internal Audit, Risk, Business & Technology Consulting

Impact Summary

Web application assessments are goal-driven exercises where an outside party attempts to understand and emulate a real-world attacker in order to obtain specific objectives such as data or system access. Source code review is a technical coding review where the outside party is provided with the application source code in order to identify coding flaws and verify that best practices are followed. Protiviti worked with CFX to establish the following goals and targets for this assessment:

1. Bypass authentication controls or gain unauthorized access to the in-scope application. **(Not Achieved)**
2. Escalate privileges on the application from a lower privileged user role. **(Not Achieved)**
3. Gain access to web application host systems or the internal network. **(Not Achieved)**
4. Gain access to sensitive information that directly enables the compromise of an end user. **(Not Achieved)**

Summary of Results

During this security assessment, Protiviti discovered one (1) High, one (1) Medium, and eight (8) Low priority vulnerabilities. Additionally, the team discovered two (2) Informational issues.

The following are issues rated as High or Medium identified during the assessment:

Web Application Assessment

• **Input Sanitization**

Source Code Assessment

• **Hardcoded Sensitive Information**

Internal Audit, Risk, Business & Technology Consulting

Strategic Recommendations

The following high-level recommendations are provided to help mitigate the risks identified in this report.

- **Application Security Architecture and Ongoing Analysis:** Perform ongoing testing of web applications prior to release on a quarterly basis.

- **Enhance Secure Coding Practices and Input Validation:** Continue to educate developers to follow secure coding best practices and techniques with a specific emphasis on input validation and output sanitization.

- **Incorporate Security into the SDLC:** Security guidelines, such as OpenSAMM, should be incorporated into the Software Development Life Cycle (SDLC) process including defining security requirements for developed applications.

It should be noted that many of Protiviti's recommendations contain instructions for specific system configuration changes (e.g., version upgrade). All recommendations should be properly evaluated and tested in a non-production environment prior to implementation on production systems. The detailed findings matrix contains a listing of findings and recommendations for this project.

 Internal Audit, Risk, Business & Technology Consulting

Face the Future with Confidence

protiviti®

E.

Annual Review and Approval of the Audit Committee Charter

CENTRAL FLORIDA EXPRESSWAY AUTHORITY BOARD
AUDIT COMMITTEE CHARTER

PURPOSE
The Audit Committee's primary function is to assist the CFX Board in fulfilling its oversight responsibilities by reviewing the financial information, systems of internal control which Management has established, the audit process, the process for monitoring compliance with laws and regulations and the Code of Ethics. In doing so, it is the responsibility of the Audit Committee to provide an open avenue of communication between the CFX Board, Management, the Internal Auditor, and external auditors. The Audit Committee is provided specific authority to make recommendations to the Chief Financial Officer, the Executive Director and the CFX Board.

ORGANIZATION
The Audit Committee shall be composed of the following voting members:

1. Orange County staff member or citizen representative appointed by the Orange County Commission or in accordance with Orange County's policies providing for appointments to other governmental agencies;
2. City of Orlando staff member or citizen representative appointed by the City of Orlando Commission or in accordance with the City of Orlando's policies providing for appointments to other governmental agencies;
3. Lake County staff member or citizen representative appointed by Lake County Commission or in accordance with Lake County's policies providing for appointments to other governmental agencies;
4. Osceola County staff member or citizen representative appointed by the Osceola County Commission or in accordance with Osceola County's policies providing for appointments to other governmental agencies;
5. Seminole County staff member or citizen representative appointed by the Seminole County Commission or in accordance with Seminole County's policies providing for appointments to other governmental agencies.
6. Brevard County staff member or citizen representative appointed by the Brevard County Commission or in accordance with Brevard County's policies providing for appointments to other governmental agencies.
7. Up to three (3) citizen representatives appointed by the CFX governing Board after receiving nominations submitted by the gubernatorial Board appointees. The term for such appointments shall be for two years commencing upon appointment which term may be renewed. One nomination per gubernatorial appointee is allowed, but it shall not be mandatory that nominations be made.

Committee member appointments may not be delegated. The Committee members will serve at the pleasure of their respective jurisdictions. County and City appointments may include contract personnel currently providing services to the appointing entity. Notwithstanding the two year term, the citizen representatives shall serve at the pleasure of the CFX Board. Committee members should have financial expertise in general accounting principles and experience reviewing financial statements and audit reports.

CHAIRMAN SELECTION

The Audit Committee will be chaired on an annual, rotating basis beginning September 1, 2017, in the following order:

> a.) Seminole County Representative
> b.) Osceola County Representative
> c.) One of Citizen Representatives
> d.) Lake County Representative
> e.) City of Orlando Representative
> f.) Brevard County Representative
> g.) Orange County Representative

The Audit Committee Chair shall serve as the Board Liaison and may be requested to attend CFX Board meetings.

In the event there is no available representative from the entity assigned to serve the role of Chairman, the next scheduled representative shall serve a one-year term with regular order of succession to resume thereafter.

SUPPORT STAFF

The Internal Audit Director and the external auditors shall have direct and independent access to the Audit Committee and individually to members of the Audit Committee. The Committee shall have unrestricted access to employees and relevant information. The Committee may retain independent counsel, accountants or others to assist in the conduct of its responsibilities, subject to the CFX procurement policy.

MEETINGS

The Audit Committee shall meet at least quarterly. Meetings may be called by the CFX Board Chairman, the Audit Committee Chair, or any two Committee members. Public notice shall be provided in accordance with State law.

The agenda will be prepared by the Internal Audit Director and approved by the Chair and provided in advance to members, along with appropriate briefing materials. In the absence of any objection, the Chair or any Committee member may add or subtract agenda items at a meeting. In the event of objection, a majority vote shall decide. The Committee meeting minutes and any Committee recommendations shall be submitted to the CFX Board for consideration.

QUORUM

If all three gubernatorial Board members make nominations and the Board approves the appointments, the Committee shall consist of nine members and a quorum shall be five members present. If only two appointments are made the Committee shall consist of eight members and a quorum shall be five members present. If only one appointment is made the Committee shall consist of seven members and a quorum shall be four members present. In order for any action or recommendation to pass there must be a majority affirmative vote of the quorum based on the then current composition of the Committee.

Due to scheduling conflicts or illness a Committee Member may appear by telephone and vote on agenda items where a quorum is physically present not to exceed three meetings per calendar year. The participating absent member must be able to hear all participants in the meeting and be heard by all participants.

RESPONSIBILITIES

Financial Reporting Oversight

1. Review with Management and the external auditors:
   - The annual financial statements and related footnotes;
   - The external auditors' audit of the financial statements and their report;
   - Management's representations and responsibilities for the financial statements;
   - Any significant changes required in the audit plan;
   - Information from the external auditors regarding their independence;
   - Any difficulties or disputes with Management encountered during the audit;
   - The organization's accounting principles;
   - All matters required to be communicated to the Committee under generally accepted auditing standards.
2. Review with Management, the CFX's financial performance on a regular basis.

Internal Control and Risk Assessment

3. Review with Management the effectiveness of the internal control system, including information technology security and control.
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.
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.

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.

Code of Ethics

7. Review with Management and monitor adequacy, administration, and compliance with the CFX's Code of Ethics.
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.

Internal Audit

9. Recommend to the Board the appointment or removal of the Internal Audit Director.
10. Review and approve the annual internal audit plan and all major changes to the plan.
11. Review the internal audit budget and submit to the Finance Committee.
12. Review and approve the Internal Audit Department Charter.
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.
14. Review annually the performance of the Internal Audit Director.
15. Review annually the effectiveness of the internal audit function.
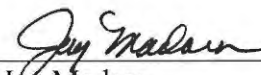
External Audit

16. Appoint an Audit Committee Member to serve on the Selection Committee for all external audit services.
17. Recommend to the CFX Board the external auditors to be appointed and the related compensation.
18. Review and approve the discharge of the external auditors.
19. Review the scope and approach of the annual audit with the external auditors.
20. Approve all non-audit services provided by the external auditors.

Other Authority and Responsibilities

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

ADOPTED this __10th__ day of October, 2019.

ATTEST: _____

Mimi Lamaute
Board Services Coordinator

_____
Jay Madara
Board Chairman

Approved as to form and legality:

_____
Diego "Woody" Rodriguez
General Counsel

F.

Internal Audit Budget for Fiscal Year 2021

Internal Audit

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

Account Number	2019 Actuals	2020 Budget	2020 YTD Actual	2020 Annualized Amt	2020 Yr. End Est	2021 Preliminary Bud
80 Other Expenses						
05 Toll Collection						
130 Administration						
690 Internal Audit						
53410 Contract Personnel	535,777.50	564,000.00	72,900.00	174,960.00	[ ]	[ ]
Total Internal Audit	535,777.50	564,000.00	72,900.00	174,960.00		
Total Toll Collection	535,777.50	564,000.00	72,900.00	174,960.00		
Total 80 Other Expenses	535,777.50	564,000.00	72,900.00	174,960.00		

		2019	2020	2020	2020	2020	2021
Account Number		*Actuals*	*Budget*	*YTD Actual*	*Annualized Amt*	*Yr. End Est*	*Preliminary Bud*
85	**Capital Expenditures**						
05	Toll Collection						
130	Administration						
690	Internal Audit						
Total	Internal Audit	0.00	0.00	0.00	0.00		
Total	Toll Collection	0.00	0.00	0.00	0.00		
Total	85 Capital Expenditures	0.00	0.00	0.00	0.00		
	Grand Total	535,777.50	564,000.00	72,900.00	174,960.00		