

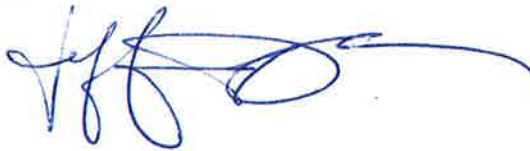
MEMORANDUM

TO: CFX Board Members

FROM: Jeff Tecau, Protiviti

DATE: April 28, 2016

SUBJECT: Internal Audit Reports



Attached, please find the 2017 Internal Audit Plan as reviewed and accepted by the Audit Committee on April 27, 2016.

The 2017 Internal Audit Plan was compiled through interviews with the Board and Authority staff. The results of the risk assessment discussions and collective insights obtained around risk trending, key changes in the organization, and key initiatives were used to develop and define a proposed listing of Internal Audit projects for 2017 to address key areas of focus. The final list of projects on the 2017 plan and the related budget allotments were discussed, selected, and approved by the Audit Committee on April 27, 2016.

Reviewed by:





*Powerful Insights.
Proven Delivery.™*

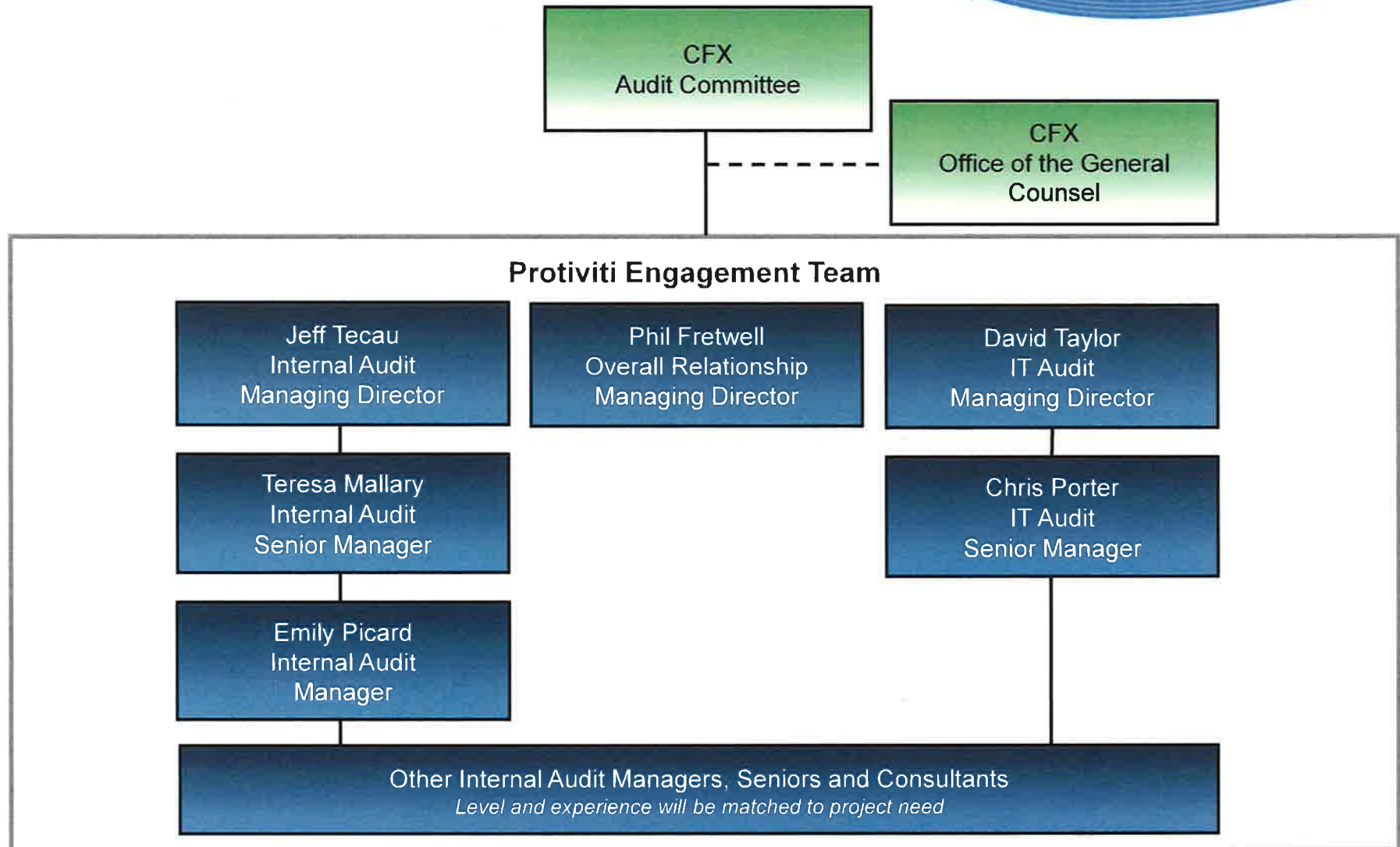
**CENTRAL
FLORIDA
EXPRESSWAY
AUTHORITY**

Internal Audit Plan For the Fiscal Year Ending June 30, 2017

protiviti®

© 2016 Protiviti Inc. All Rights Reserved. This document has been prepared for use by 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.

Your Internal Audit Team



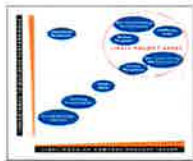
Background

A 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 2017 risk assessment was to identify and prioritize key areas of risk within the Authority to consider in designing the fiscal 2017 Internal Audit plan. The approach utilized in conducting the fiscal 2017 risk assessment and in developing the fiscal 2017 Internal Audit plan is depicted below. Risk assessment results are included in Appendix B.



Identify Key Areas of Risk to be Assessed

- Confirm and update prior year risk areas based upon review of prior year work papers, audit results, and discussions with senior management and the Board
- Determine preliminary risk ratings based upon prior year results



Assess & Prioritize Areas of Risk

- Conduct interviews with senior management and the Board to confirm and validate the current enterprise risk model to gain additional insight around risk trending, key changes in the organization, and key initiatives
- Aggregate and compile resulting information
- Provide a graphical representation of enterprise risks on a risk heat map to prioritize areas of risk



Select Focus Areas

- Evaluate the prioritized enterprise risks and management commentary to determine Internal Audit focus areas for fiscal year 2017
- Develop and define a preliminary listing of proposed Internal Audit projects to address the areas of focus



Develop & Approve Audit Plan

- Establish high-level scoping statements and levels of effort for proposed projects
- Finalize budget allotments and propose projects for Audit Committee approval
- Finalize proposed timing for selected projects
- Finalize Internal Audit plan and obtain Audit Committee approval

Interview List

The following thirty (30) individuals were interviewed to gather information to develop the fiscal year 2017 Internal Audit plan:

<u>Name</u>	<u>Title</u>	<u>Name</u>	<u>Title</u>
Commissioner Welton Cadwell	Board Chairman	Joe Passiatore	General Counsel
Commissioner Scott Boyd	Board Vice-chairman	Linda Lanosa	Deputy General Counsel
Commissioner Brenda Carey	Board Secretary/Treasurer	Claude Miller	Director of Maintenance
Mayor Buddy Dyer	Board Member	David Wynne	Director of Toll Operations
Commissioner Fred Hawkins Jr.	Board Member	Ben Dreiling	Director of Construction
Mayor Teresa Jacobs	Board Member	Joann Chizlett	Director of IT Special Projects
Andria Herr	Board Member	Glenn Pressimone	Director of Engineering
Jay Madara	Board Member	Iranetta Dennis	Director of Supplier Diversity
S. Michael Scheeringa	Board Member	Rene Rodrigue	Director of Information Technology
Brian Battles	Audit Committee Chairman	Evelyn Wilson	Director of Human Resources
Laura Kelley	Executive Director	Michael Carlisle	Manager of Accounting and Finance
Joe Berenis	Chief of Infrastructure	Don Budnovich	Resident Engineer/Sr. Project Manager
Corey Quinn	Chief of Technology/Operations	Dan Goff	Vendor; AECOM Project Manager
Lisa Lombard	Chief Financial Officer	Allie Braswell	Vendor; Egis EPASS Project Manager
Michelle Maikisch	Chief of Staff/Public Affairs	Brent Wilder	Vendor; PFM Financial Advisor

Internal Audit Spend Benchmarks

There are several qualitative factors to consider when evaluating the level of Internal Audit resources. Below are statistics from the Institute of Internal Audit (IIA) 2015 Global Audit Information Network (GAIN) Benchmarking Study for the Transportation Industry to use as a starting point and key factors to consider, based on specific needs and circumstances.

IIA Benchmark Size of Company	IIA Benchmark Average	CFX FY 2015	IIA Benchmark Average Audit Staff	IIA Benchmark Average IA Cost as % of Revenue	Average Internal Audit Cost (Calculated)
Revenues < \$500M	\$382M	\$359M	3.80	0.1133%	\$407K
Assets \$1B - \$5B	\$2.74B	\$4.4B	7.19	0.0412%	\$1.8M

Average IA Spend

Factors	Lowers Resource Need	Increases Resource Need
Number of Locations	Few locations	Significant number of locations
Degree of Centralization	Highly centralized	Decentralized
Control Environment	Strong internal control environment	Poor internal control environment
Maturity of Business Processes	Optimized processes	Ad-hoc processes
Audit Scope / Board & Mgt Needs	Limited scope	Expansive scope
Degree of Change in the Business	Low degree of change	High degree of change
Board's Risk Tolerance	High risk tolerance	Low risk tolerance
Regulations	Low	High

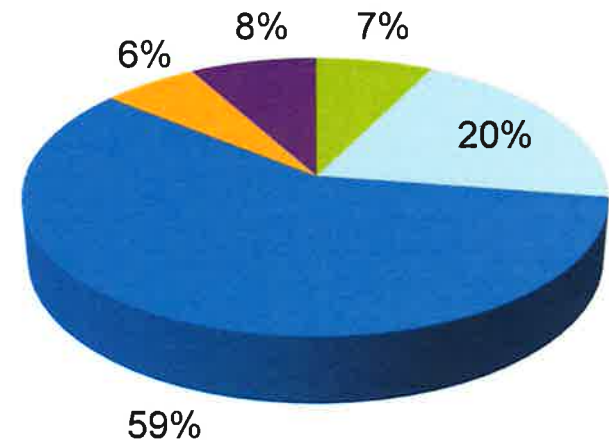
3 Year Internal Audit Plan

			Audit Plan Year		
Description	Frequency	Date Last Performed	2017	2018	2019
Annual Internal Audits					
Internal Audit Plan and Risk Assessment	Annual	2016	\$ 25,000	\$ 25,000	\$ 25,000
Board and Audit Committee Meetings	Annual	2016	\$ 15,000	\$ 15,000	\$ 15,000
Prior Year Recommendations: Semi-Annual Follow-up	Annual	2016	\$ 12,000	\$ 12,000	\$ 12,000
Procurement & Contract Billing Audits	Annual	2016	\$ 40,000	\$ 40,000	\$ 40,000
DHSMV Data Security Assessment	Annual	2016	\$ 25,000	\$ 25,000	\$ 25,000
Contingency for Special Project Requests	Annual	N/A	\$ 25,000	\$ 25,000	\$ 25,000
		Total	\$ 142,000	\$ 142,000	\$ 142,000
Cyclical Audits					
Purchasing Spend Data Audit	5 Year Cycle	2010	\$ 35,000		
Accounting System Access and SOD Review	5 Year Cycle	2011	\$ 25,000		
Human Resources Process Review	5 Year Cycle	2011	\$ 25,000		
Business Continuity Management Review	5 Year Cycle	N/A	\$ 32,000		
Information Security Risk Assessment - Phase I	3 Year Cycle	N/A	\$ 25,000	X	
Toll Violations and Toll-by-Plate Audit	5 Year Cycle	2012		X	
Ethics Policy Compliance Audit	3 Year Cycle	2015		X	
IT General Controls Review	3 Year Cycle	N/A		X	
Bond Financing Review	3 Year Cycle	2016			X
Toll Revenue Audit	3 Year Cycle	2016			X
Sensitive Data / Data Management Review	5 Year Cycle	2014			X
Safety and Maintenance Policy and Procedures Compliance Audit	5 Year Cycle	2014			X
PCard and Gas Card Audit	5 Year Cycle	N/A			X
COSO 2013 Governance Review	5 Year Cycle	2015			X
Right of Way Audit	5 Year Cycle	2016			X
As Needed Audits					
Public Records Review	As Needed	N/A	\$ 30,000		
Change Management Review – Tolling System Replacement	As Needed	2016 - Phase I	\$ 50,000		
Customer Service Center Performance Assessment	As Needed	2015	\$ 48,000		
Call Center Staffing Model Development	As Needed	N/A	\$ 15,000		
Vendor Security Review	As Needed	N/A	\$ 48,000		
Discount/Rebate Program Audit	As Needed	N/A	\$ 24,000		
Internal Penetration Test	As Needed	N/A		X	
ISO 27001 Information Security Review	As Needed	N/A		X	
Swaps Review	As Needed	N/A		X	
TRAILS Program Review	As Needed	N/A		X	
IT Service Management Review	As Needed	N/A			X
Customer Service Management and Lane Scheduling Review	As Needed	N/A			X
		Grand Total	\$ 499,000	TBD	TBD
PCI Assessment					
PCI Assessment with Report on Compliance	Annual	2015	\$ 65,000	\$ 65,000	\$ 65,000

© 2016 Protiviti Inc. All Rights Reserved. This document has been prepared for use by 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.

FY 2017 Internal Audit Coverage

Strategic & Governance	Budget Allocation	Frequency
• Fiscal 2018 Internal Audit Plan and Risk Assessment	\$25,000	Annual
• Prior Audit Recommendations: Semi-Annual Follow-up	\$12,000	Annual
Financial		
• Procurement & Contract Billing Audits	\$40,000	Annual
• Purchasing Spend Data Audit	\$35,000	5 Year Cycle
• Accounting System Access and SOD Review	\$25,000	5 Year Cycle
Operations & IT		
• DHSMV Data Security Assessment	\$25,000	Annual
• Human Resources Process Review	\$25,000	5 Year Cycle
• Business Continuity Management Review	\$32,000	5 Year Cycle
• Information Security Risk Assessment – Phase I	\$25,000	3 Year Cycle
• Change Management Review – Tolling System Replacement	\$50,000	As Needed
• Customer Service Center Performance Assessment	\$48,000	As Needed
• Call Center Staffing Model Development	\$15,000	As Needed
• Vendor Security Review	\$48,000	As Needed
• Discount/Rebate Program Audit	\$24,000	As Needed
Regulatory & Compliance		
• Public Records Review	\$30,000	As Needed
Other		
• Board and Audit Committee Meetings	\$15,000	Annual
• Contingency for Special Project Requests	\$25,000	Annual
Total Internal Audit Budget	\$499,000	
 PCI Assessment with Report on Compliance*	 \$65,000*	 Annual
GRAND TOTAL	\$564,000	



* The PCI Assessment is a separate contract and is not included in the Internal Audit contract

Internal Audit Timeline

FY 2017 Estimated Project Timeline

July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June
------	-----	------	-----	-----	-----	-----	-----	-----	-----	-----	------

Annual Audits

1. Internal Audit Plan and Risk Assessment
2. Board and Audit Committee Meetings
3. Prior Audit Recommendations: Semi-Annual Follow-Up
4. Procurement & Contract Billing Audits
5. DHSMV Data Security Assessment
6. Contingency for Special Project Requests

Cyclical Audits

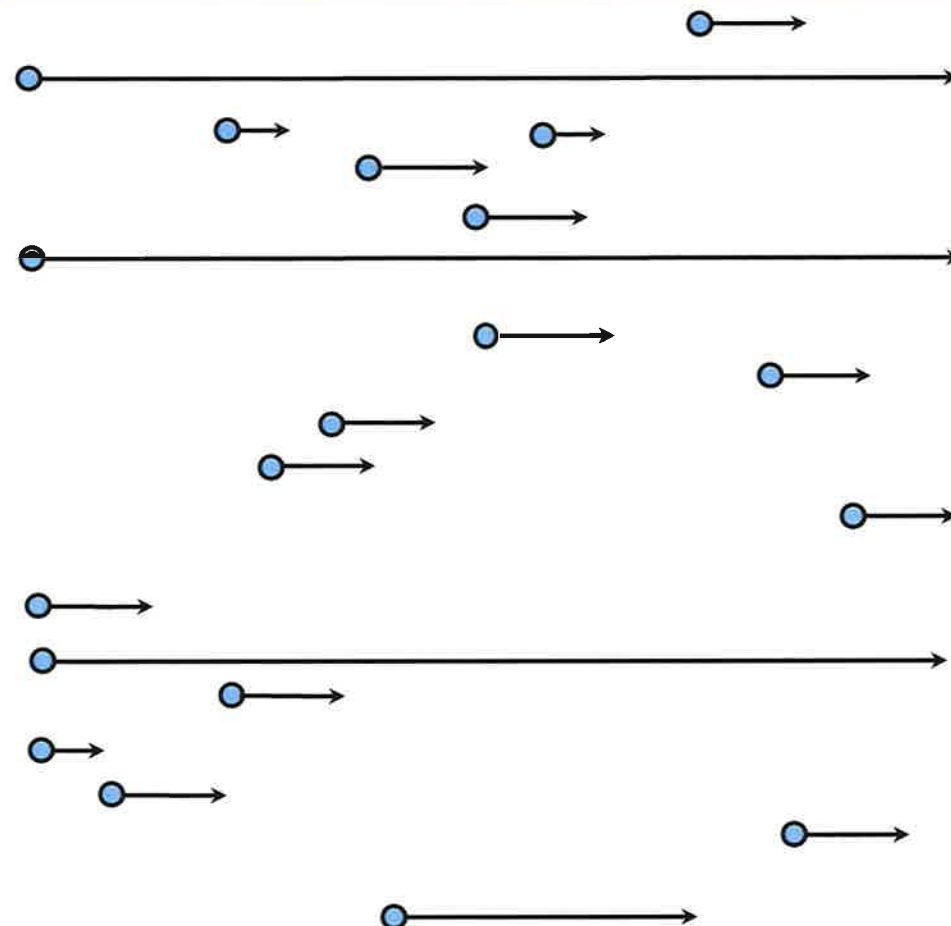
6. Purchasing Spend Data Audit
7. Accounting System and SOD Review
8. Human Resources Process Review
9. Business Continuity Management Review
10. Information Security Risk Assessment – Phase I

As Needed Audits

11. Public Records Review
12. Change Management Review – Tolling System Replacement
13. Customer Service Center Performance Assessment
14. Call Center Staffing Model Development
15. Vendor Security Review
16. Discount / Rebate Program Audit

PCI Assessment

17. PCI Assessment with Report on Compliance



protiviti[®]

FY 2017 Internal Audit Project Descriptions

#	Project	Project Description	Risks	Estimated Cost
1	Internal Audit Plan and Risk Assessment (Annual)	We will conduct a risk assessment to highlight the Authority's current year risk profile, to identify risk trends, and to form the foundation for the fiscal year 2017/2018 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 2017/2018 Internal Audit plan, with a focus on addressing opportunities identified during the risk assessment process.	Strategic Planning Fraud Governance	\$25,000
2	Board and Audit Committee Meetings (Annual)	Protiviti will attend Board meetings and prepare for and present at all Audit Committee meetings during fiscal year 2017. This includes document preparation time and preparation time with management and the Audit Committee in advance of meetings.	Governance	\$15,000
3	Prior Audit Recommendations: Semi-Annual Follow-up (Annual)	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	\$12,000
4	Procurement & Contract Billing Audits (Annual)	This audit will encompass a selection of 2 or 3 large engineering, construction, maintenance, operations, or legal contracts on an annual, rotational basis, with the objective of verifying that internal controls are in place to ensure work performed under large contracts has been billed in accordance with contractual terms and conditions. The work will include testing pricing and hours worked for accuracy and validity, testing invoice approvals, testing vendor compliance with other contractual obligations, using data analytics to identify high risk vendors and/or change orders, and review of other key data points.	Contract Management Contract Performance Reporting Cost Containment Procurement and Vendor Selection	\$40,000
5	DHSMV Data Security Assessment (Annual)	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 Security Data Security	\$25,000
6	Contingency for Special Project Requests (Annual)	Contingency in Internal Audit budget for special project requests.	Various	\$25,000
7	Purchasing Spend Data Audit (Cyclical)	This review will focus on a 100% interrogation of spending data over a 3 year history to identify opportunities for recovery such as vendor overpayments, unused vendor credits, etc. We will use our proprietary tools to review the 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	\$35,000

© 2016 Protiviti Inc. All Rights Reserved. This document has been prepared for use by CFX's management, audit committee and board of directors.

8 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.

FY 2017 Internal Audit Project Descriptions

#	Project	Project Description	Risks	Estimated Cost
7	Accounting System Access and Segregation of Duties Review (Cyclical)	The financial close and related accounting processes will be reviewed for appropriate segregation of duties among Authority 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	\$25,000
8	Human Resources Process Review (Cyclical)	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 will be reviewed and compared to leading practices.	Human Resources Succession Planning	\$25,000
9	Business Continuity Management Review (Cyclical)	This review will focus on how the Authority 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).	Business Continuity	\$32,000
10	Information Security Risk Assessment – Phase I	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 conducted in two phases, Phase I taking place in FY 2017.	Cyber Security Data Security	\$25,000
11	Public Records Review (One-Time)	This review will focus on the Authority's records management processes and policies to comply with public records laws. Data retention surrounding electronic communications via email, mobile, and voice mail will also be reviewed to identify the technology needed to assist with capturing and retaining data from such communication. Additionally, we will review documentation retention schedules specific to document classification (different types must be kept for a different lengths of time) for consistency with rules established by the Florida Secretary of State.	Records Management	\$30,000

FY 2017 Internal Audit Project Descriptions

#	Project	Project Description	Risks	Estimated Cost
12	Change Management Review –Tolling System Replacement (One-Time)	The Authority is in the process of replacing the toll plaza collection system. An access control review will be conducted on the Law Enforcement Notification System ("LENS") component of this replacement. Additionally, network vulnerability scans may be conducted on systems that have completed Factory Acceptance Testing but have not been put into production. This will allow Internal Audit to identify potential vulnerabilities to systems prior to their deployment so they may be remediated.	IT Change Management Toll Collections	\$50,000
13	Customer Service Center Performance Assessment (One-Time)	If the Authority does not move to a centralized customer contact center back office, Protiviti subject matter experts will conduct a re-audit of the contact center to follow-up on an audit conducted during fiscal 2015. A new vendor is overseeing the operation as of July 1, 2015. The re-audit will involve a deep-dive review of progress toward the implementation of each prior audit recommendation as well as a comparison of the new vendor's performance against benchmarks and other leading practices through silent observations of calls and statistical analysis to extrapolate results.	Back Office Consolidation Cost Containment Customer Satisfaction Public Relations	\$48,000
14	Call Center Staffing Model Development (One-Time)	CFX has asked for assistance with an independent analysis of their call center staffing numbers and for help forecasting agent needs to assist them with managing their vendor contract and higher than normal call volumes that are exceeding their current contract limitations.	Cost Containment Customer Satisfaction Public Relations	\$15,000
15	Vendor Security Review (One-Time)	This review will assess the security of vendor IT connections that come into the Authority's environment, as well as the design and operating effectiveness of the security configurations and controls that surround the Authority's data within vendor's environments.	Cyber Security Data Security	\$48,000
16	Discount/Rebate Program Audit	Given recent changes to provide more volume discounts to riders as a relief measure with the interstate construction project underway in addition to the new marketing initiatives underway, rebates and volume discounts continue to increase. This project would involve an audit of rebates and volume discount programs for completeness and accuracy and a review of the policies and procedures in place to manage the process.	Toll Collections Toll Discounts/Rebates	\$24,000



FY 2017 PCI Assessment

#	Project	Project Description	Risks	Estimated Cost
1	PCI Assessment with Report on Compliance	This project will be to fully test the Authority's compliance with the PCI Data Security Standard, (PCI-DSS) version 3.1 and issue a Report on Compliance (ROC). The testing will cover all twelve sections of the PCI-DSS.	IT Security	\$65,000



Appendix A

Internal Audit Charter

© 2016 Protiviti Inc. All Rights Reserved. This document has been prepared for use by CFX's management, audit committee and board of directors.

12 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®



Internal Audit Charter

Central Florida Expressway Authority Fiscal 2017 Internal Audit Department Charter

**Proposed changes to Fiscal 2017 Internal Audit Charter are italicized*

MISSION

The mission of the internal audit department is to provide the Authority Board with unbiased, objective assessments of whether Expressway resources are responsibly and effectively managed to achieve intended results.

PURPOSE

Internal audit's purpose is to add value, improve operations, and enhance transparency. It 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.

INDEPENDENCE

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 Office of the General Counsel. To ensure independence, the internal audit function has no direct responsibility or any authority over any of the activities or operation of the Expressway. *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 not be unduly influenced by their own interests or by others in forming judgments.*



Internal Audit Charter

AUTHORITY

Everything the Expressway Authority does is subject to assessment by internal audit. Internal Audit shall have full, free, and unrestricted access to all activities, records, properties and personnel. The Internal Auditor shall have direct and independent access to the Audit Committee and individually to members of the Audit Committee. The internal audit department is authorized to allocate resources, set frequencies, select subjects, determine scopes of work for projects as approved by the Audit Committee, and apply the techniques required to accomplish audit objectives. In addition, the Internal Auditor may obtain the necessary assistance of personnel in units of the organization where they perform audits, as well as other specialized services from within or outside the organization, as approved by the Audit Committee.

SCOPE

Management is responsible for establishing and maintaining risk management, control, and governance processes. The scope of work of internal audit is to determine whether management's processes are adequate and functioning in a manner to ensure:

- Risks are appropriately identified and managed.
- Interaction with the various governance groups occurs as needed.
- Significant financial, managerial, and operating information is relevant, reliable and understandable.
- Employee actions comply with policies, standards, procedures, and applicable laws and regulations.
- Resources are acquired economically, used efficiently, and adequately protected.
- Programs, plans, and objectives are achieved.
- Quality and continuous improvement are fostered in control processes.
- Significant legislative or regulatory issues are recognized and addressed properly.

Internal Audit Charter

RESPONSIBILITY

The internal audit department's responsibility includes, but is not limited to:

- Develop a flexible annual audit plan using appropriate risk-based methodology, including any risks or control concerns identified by management, and submit that plan to the Audit Committee for review and approval.
- Implement the annual audit plan, as approved, including, and as appropriate, any special tasks or projects requested by management and the Audit Committee.
- Maintain a professional audit staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of this Charter.
- Establish a quality assurance program by which the Internal Auditor assures the operation of internal auditing activities.
- Perform consulting services, beyond internal audit's assurance services, to assist management in meeting its objectives. Examples may include facilitation, process design, training, and advisory services.
- Evaluate and assess significant merging/consolidating functions and new or changing services, processes, operations, and control processes coincident with their development, implementation, and/or expansion.
- Issue periodic reports to the Audit Committee and management summarizing results of audit activities as well as results of internal and external assessments conducted in association with the Quality Assurance and Improvement Program.
- Keep the Audit Committee informed of emerging trends and successful practices in internal auditing.
- Provide a list of significant measurement goals and results to the Audit Committee.
- Assist in the investigation of significant suspected fraudulent activities within the organization and notify management and the Audit Committee of the results.
- Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to the organization at a reasonable overall cost.



Internal Audit Charter

STANDARDS & PROFESSIONALISM

Internal audit shall comply with the International Standards for the Professional Practice of Internal Auditing of The Institute of Internal Auditors. Consistent with the IIA Standards, internal audit recognizes the mandatory nature of the Definition of Internal Auditing, the Code of Ethics, and the IIA Standards. *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.*



Appendix B

Enterprise Risk Assessment

© 2016 Protiviti Inc. All Rights Reserved. This document has been prepared for use by CFX's management, audit committee and board of directors.

17 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®

Enterprise Risk Assessment

To assist with the development of the fiscal 2017 Internal Audit Plan, Internal Audit used prior years' risk models and risk trending data as the starting point for discussions with the Board and management. Internal Audit asked the Board and 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 the Board and management and from risk surveys of management to develop a list of potential internal audit projects for fiscal 2017, 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 the Authority 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 2017 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.

CFX Risk Model

Strategic & Governance

- **Strategic Planning**
- Regulatory Changes
- **Governance**
- Communication
- **Back Office Consolidation**
- **Public Relations**
- Organization Structure
- Statewide Interoperability
- Political Environment
- Leadership
- National Interoperability
- Asset & Liability Transfer Risk*
- **Succession Planning**
- Access to Capital
- Ethical Compliance
- Outsourcing
- Toll Rate Management

Financial

- **Financial Reporting**
- **Cost Containment**
- Management Performance Reporting
- **Fraud**
- Bond Financing / Covenant Compliance
- Swap Pricing*
- **Contract Performance Reporting**
- **Procurement and Vendor Selection**
- Right of Way
- Cash Handling
- Treasury and Liquidity Management

Operations & IT

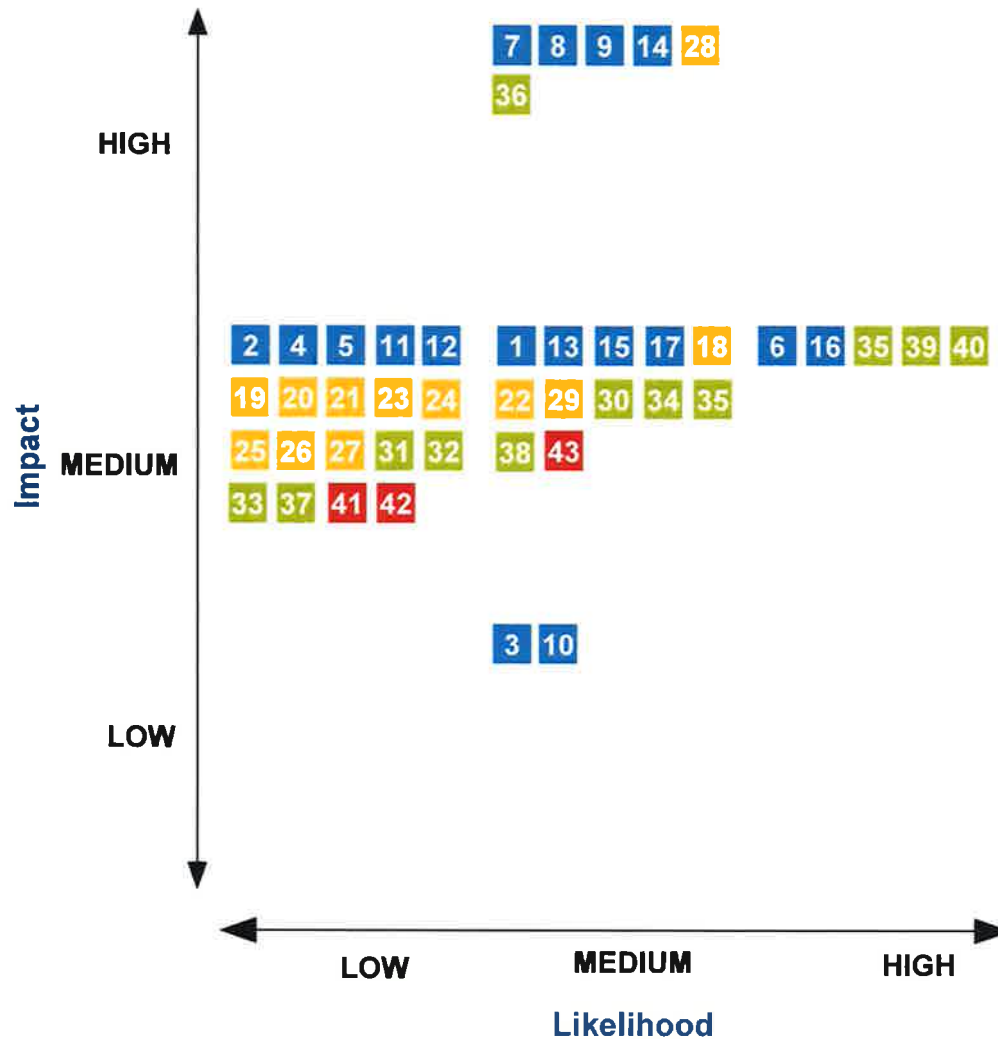
- Toll Violations
- **Toll Collections**
- **Data Security***
- IT Applications
- **Human Resources**
- **Customer Satisfaction**
- **IT Infrastructure / Business Continuity**
- **Cyber Security***
- **Toll Discounts/Rebates***
- **IT Change Management**
- Insurance Coverage

Regulatory & Compliance

- Maintenance & Safety
- **Records Management**
- **Contract Management**

* Represents new risks added for FY 2017. **Bold** represents risks addressed by FY 2017 Internal Audit plan.

Enterprise Risk Map – Residual Risk



STRATEGIC & GOVERNANCE

- 1 Strategic Planning
- 2 Organization Structure
- 3 Succession Planning
- 4 Regulatory Changes
- 5 Access to Capital
- 6 Statewide Interoperability
- 7 Governance
- 8 Political Environment
- 9 Ethical Compliance
- 10 Communication
- 11 Leadership
- 12 Outsourcing
- 13 Public Relations
- 14 Back Office Consolidation
- 15 National Interoperability
- 16 Toll Rate Management
- 17 Asset & Liability Transfer Risk

OPERATIONS & IT

- 30 Toll Violations
- 31 Toll Collections
- 32 IT Application Controls
- 33 Human Resources
- 34 IT Infrastructure/Business Continuity
- 35 Cyber Security
- 36 IT Change Management
- 37 Insurance Coverage
- 38 Customer Satisfaction
- 39 Data Security
- 40 Toll Discounts/Rebates

REGULATORY & COMPLIANCE

- 41 Contract Management
- 42 Maintenance and Safety
- 43 Records Management

FINANCIAL

- 18 Bond Financing / Covenant Compliance
- 19 Fraud
- 20 Management Performance Reporting
- 21 Budgeting
- 22 Cost Containment
- 23 Treasury and Liquidity Management
- 24 Cash Handling
- 25 Procurement and Vendor Selection
- 26 Contract Performance Reporting
- 27 Financial Reporting
- 28 Right of Way
- 29 Swap Pricing

Key Fraud Risks

As part of the Enterprise Risk Assessment, Internal Audit discussed potential fraud risk scenarios with management and the Board and identified the following potential fraud scenarios for consideration when executing FY 2017 Internal Audit work.

- Unauthorized / improper use of corporate credit cards / misuse of funds
- Awarding of work to related parties
- Bribery / kickback to award bids
- Management disclosure of confidential information during procurement
- Theft or misuse of confidential financial information
- Billing for work not performed or vendor overbillings
- Circumvention of procurement
- Selective disclosure to Board or public
- Earnings management
- Management override of controls
- Nepotism
- Use of confidential information for personal gain
- Solicitation
- Unauthorized adjustment of salary / wages
- Creation of ghost vendors or employees
- Manual journal entries
- Partner billings / payments
- Adjustment to customer accounts
- Theft of cash
- Toll violations
- Counterfeit cash
- Price fixing
- Bid rigging
- Off contract agreements
- Payment of false invoices / invoices do not match contract terms
- Misuse of company assets / theft of company assets
- Falsification of hours worked
- Theft / forgery of payroll or blank checks



Appendix C

Other Potential Audits

Other Potential Audits

#	Project	Project Description	Risks	Estimated Cost
1	Toll Violations and Toll-by-Plate Audit	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	\$40,000
2	Ethics Policy Compliance Audit	CFX has a formal ethics policy in place and will update it to incorporate new ethics language imposed by Florida state legislation. Later in the year, 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 Behavior Financial Reporting	\$29,000
3	IT General Controls Review	This review will focus on the 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.	IT Infrastructure Application Controls Change Management	\$36,000
4	Bond Financing Review	The Authority has \$2.5B 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	\$40,000
5	Toll Revenue Audit	This audit will focus on cash toll collections and electronic tolling collections, with the objectives to review (1) controls exist to ensure 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, and (4) appropriate monitoring and measurements are in place to review toll revenue. Additionally, IT general controls around supporting systems and information technology will be reviewed. Additionally, we may review the Authority's process for determining the ways to structure tolls (e.g. toll rates by axles vs flat rates, variable rate tolling, time of day tolling). We may also provide recommendations for enhancements to the structure, if in scope.	Toll Collections Cash Handling	\$75,000

Other Potential Audits

#	Project	Project Description	Risk	Estimated Cost
6	Sensitive Data / Data Management Review	The objectives of the project will be to identify if sensitive data is inappropriately stored in locations on the CFX network - in violation of company policy and leading practices. In addition, we will perform a high-level evaluation of the controls over the sensitive data repositories that are identified (if applicable) to determine if potential gaps exist.	Cyber Security Data Security	\$40,000
7	Safety and Maintenance Policy and Procedures Compliance Audit	The objective of this project will be to review the safety policies and procedures in place, including any recent technological enhancements to safety within the system (e.g. new technology measures to help prevent wrong way driving), and to test compliance with the safety policies.	Maintenance and Safety	\$30,000
8	P-Card and Gas Card Audit	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	\$20,000
9	COSO 2013 Governance Review	This audit will focus on the testing of CFX's governance internal controls identified as part of the COSO 2013 governance review conducted in FY 2015. In addition, we may assist with implementing certain recommendations from the COSO 2013 review performed in FY15; specifically, developing a checklist for the Board and Board committees to be used to manage compliance with identified requirements from respective charters and the CFX ethics policy.	Governance Ethical Compliance	\$25,000
10	Right of Way Audit	Review the processes in place to procure Right of Way legal counsel. Identify the mix of in-house vs outsourced work. Review in-house legal invoice review procedures for ROW services for tasks and billings. Review the contracted rate structure for appraisal work (use of caps, mix of variable v fixed fees). 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	\$30,000
11	Internal Penetration Test	Protiviti will assess the security of internal networks, devices, and servers as part of an internal penetration test. This test will identify risks to those networks, devices, and servers posed by outdated software, missing patches, or insecure configurations. Attempts will then be made to exploit these vulnerabilities with manual techniques.	Cyber Security Data Security	\$32,000

Other Potential Audits

#	Project	Project Description	Risk	Estimated Cost
12	ISO 27001 Information Security Review	This review will compare CFX's information security practices and procedures to the ISO 27001 framework. This framework is widely recognized as the benchmark for assessing / creating overall information security programs. Protiviti will utilize an adapted version of the Carnegie Mellon Capability Maturity Model (CMM) to report on the results. The CMM helps to identify critical areas that must be addressed before an organization can progress to a more mature state.	Cyber Security Data Security	\$45,000
13	Swaps Review	<p>Currently, five forward-stating, variable-to-fixed rate interest rate swap agreements exist covering approximately \$499K of outstanding debt. These agreements were entered into on July 13, 2004. The existing synthetic fixed rate swap agreements cover approximately 19% of the overall portfolio, below the existing 25% cap set by Board policy. A review of the existing swap agreements would entail a look back analysis of the transactions supporting the existing swap arrangements on the books. The review would be performed by an independent, third party hired by procurement, with a first phase to outline historical facts and information (to the extent it exists) around the following:</p> <ul style="list-style-type: none"> - Advice provided to the former CFX Board for consistency with available market data at the time the swap arrangements were entered into; -Review of the terms associated with the agreements (features, etc.) and communications around such by the Financial Advisor that advised CFX on the existing arrangements; and -Review of market rates and pricing of the swaps compared to available market data at the time. <p>CFX continues to consult with its Financial Advisor and Finance Committee to review available options specific to amending or terminating the existing swap arrangements and should consider this as a potential project only if the Audit and Finance Committees believe it valuable.</p>	Swap Pricing	* To be determined through a formal RFP process
14	TRAILS Program Review	This audit will encompass a review of the policies and procedures for new tolling lanes on the system that is expected to sell transponders, handle a higher volume of cash than the traditional lanes, process credit cards, and handle checks.	Cash Handling	\$20,000

Other Potential Audits

#	Project	Project Description	Risk	Estimated Cost
15	IT Service Management Review	This review will focus on IT operational effectiveness and entail the following: (1) Processes for receiving, responding to and prioritizing requests for work; (2) Program and project management procedures and governance entities; (3) Review of overall roles and responsibilities for alignment with technology strategy and business objectives; (4) Review of IT service management procedures (potentially using ITIL); (5) Analyze the procedures for communication and transparency of IT projects and effectiveness; (6) Compare with leading practices, evaluate maturity, and provide specific recommendations for effectiveness/ efficiency.	IT Infrastructure IT Applications Strategic Planning Communication	\$50,000
16	Customer Service Management and Lane Scheduling Review	Protiviti will review the use of scheduling toll collectors on the system, lane management, and use of traffic studies to drive scheduling by URS/AECOM in relation to customer service impact.	Customer Satisfaction	\$25,000