METRO | MEMORANDUM

To: Terry Mitchell, Chair, Finance, Audit & Administrative (FAA) Committee
Wade Cooper, Member, FAA Committee
Eric Stratton, Member, FAA Committee
Sabino Renteria, Member, FAA Committee

CC: Randy Clarke, President/CEO

From: Terry Follmer, CPA, MBA, CIA, CISA, CISSP
VP, Internal Audit

Date: October 9, 2019

Subject: **Approved FY2020 Internal Audit Plan**

Purpose

This proposed Capital Metro Internal Audit Plan (Audit Plan) summarizes the planning methodology and the audit projects that Internal Audit recommends performing during FY2020.

FY2020 Audit Plan & Updates

The Institute of Internal Auditor's (IIA) *International Standards for the Professional Practice of Internal Auditing* require that risk-based plans be developed to determine the priorities of the internal audit activity, consistent with the organization's goals.

The proposed FY20 Internal Audit Plan (Table 1) was developed by performing a comprehensive risk assessment. This included a risk assessment survey sent to management and Board members, management interviews, and discussions with Board members. Additionally, we collaborated and reviewed the audit plans of VIA in San Antonio, METRO in Houston, and DART in Dallas. The Internal Audit Department also reviewed prior external consulting and audit reports (e.g. FTA Triennial, Quadrennial), operating and capital budgets, organization charts, and the Strategic Plan to help ensure other potential risk and opportunity areas were identified and proposed projects are aligned to address the strategic risks of the Authority.

Based upon the results of the risk assessment, the FY20 Plan has a stronger focus on IT security, Project Connect, Positive Train Control expenditures, financial controls and the service providers. The proposed plan includes four IT projects which includes a formal assurance review of endpoint management (e.g. patching, configuration management, etc.) of computers/servers, the Annual Cybersecurity Review (i.e. IT Penetration and Vulnerability Assessment), NIST Cybersecurity Framework facilitated self-assessment, and an IT review of

Rail Systems Security. On the financial side there is a project testing the SOX like controls over the payroll cycle. Other projects to highlight from the FY20 Plan include the Quadrennial Review which is a state-mandated performance audit, the Quality Assessment Review of the Internal Audit Department that is required every three years, and the audit of the DBE Program. Internal Audit believes these focus areas together with the other projects in the proposed Audit Plan will appropriately address the risks identified.

The FY20 audit plan also includes a list of contingent projects (Table 2) that will serve as backup projects that will be performed if the original plan is running ahead of schedule or if some of the projects must be delayed or cancelled. Furthermore, the Audit Plan is meant to be a risk based flexible audit plan so as emerging risks arise or priorities change, the Internal Audit Department will bring these future project changes to management and the FAA Committee for approval.

Internal Audit Project Staffing

Staffing for the FY20 Audit Plan will use a combination of internal and external resources to perform the projects. Historically the Internal Audit Department has issued approximately seven audit assurance projects per year. The FY20 plan includes eleven assurance projects and six advisory projects, and Internal Audit believes these additional projects can be completed through better planning, scoping and coordination with management. The department is currently fully staffed with three full time auditors, and we continue to mature the UT Audit Intern program started last year. This Fall semester we will have twelve graduate Accounting students from UT's #1 ranked Masters of Professional Accounting program who will be assisting on three projects as part of their required Audit class. This is our third semester participating in this highly successful program, and we plan on continuing the Audit Intern program with a fresh class in the Spring. Each student in the intern program is providing up to 60 hours of project time for the semester as part of their Audit class at UT. Additionally, the Annual Cybersecurity Review (i.e. IT Penetration and Vulnerability Assessment), and an IT review of Rail Systems Security will be joint projects funded by the IT Department. We believe this mix of internal and external resources is sufficient to perform the projects listed in the FY2020 Audit Plan (see Table 1).

Professional Requirements & Auditor Independence

The Internal Audit Department conducts our audits in conformance with Generally Accepted Government Auditing Standards promulgated by the Comptroller General of the United States and the IIA's International Standards for the Professional Practice of Internal Auditing and Code of Ethics. These standards require that we be independent from any entity or person that we audit or may audit and be objective when conducting such audits. Furthermore, IIA Standard 1110 requires that the CAE confirm to the board, at least annually, the organizational independence of the internal audit activity. Capital Metro Internal Audit is organizationally independent of management and, as such, remains objective when conducting audits, and our staff have no conflicts of interest with the proposed FY20 Audit Plan.

TABLE 1 – FY2020 Audit Assurance & Advisory Projects

	Audit Project	**Risk Area**	**Audit Type**	**Audit Objective & Scope**	**Estimated Hours**
1	Semiannual Implementation Status Updates - November 2019	Compliance	Assurance	Monitor and report on implementation status of previously agreed-upon corrective action plans (CAPs). Status updates are performed twice each year (Spring and Fall.)	160
2	Semiannual Implementation Status Updates - May 2020	Compliance	Assurance	Monitor and report on implementation status of previously agreed-upon corrective action plans (CAPs). Status updates are performed twice each year (Spring and Fall.)	160
3	FY2020 Risk Assessment & FY2021 Audit Plan Development	Governance	Continuous Improvement & QC	Develop the annual risk based internal audit services plan to identify audit and non-audit projects and effectively allocate resources. Update and align the plan with changing organizational risks/opportunities.	300
4	Quadrennial Review	Strategic & Regulatory	Continuous Improvement & QC	State-Mandated Performance Audit	*300*

5	QAR (Quality Assurance Review) of Internal Audit practices	Quality Control & Assurance	Continuous Improvement & QC	Complete FY2021 external Quality Assurance Review: GAGAS requires an external peer review at least once every 3 years. The external review is due by October 31, 2020.	*320*
6	SOX Like Key Financial Control Testing	Financial	Assurance	Payroll process - review design and operating effectiveness of controls	200
7	Project Connect - System Controls & Processes (e-Builder)	Strategic & Technology	Assurance	Configuration and mgt of e-Builder system. A cloud based end-to-end Project Management Information Solution (PMIS) delivering outcomes from capital planning and design through commissioning.	320
8	Project Connect - Marketing & Planning Expenditures	Strategic & Regulatory	Assurance	After firm is selected and Media Plan is developed, audit invoices to ensure contract and regulatory compliance.	240
9	Fixed Route Bus Contract Change Over - Inspections & Final Settlements	Operations	Assurance	Review process and controls related to the Bus contract change over including work performed and final settlement payments.	300
10	PTC (Positive Train Control) - Expenditures & Drawings	Strategic & Regulatory	Assurance	Review billings and support for compliance with contract terms and conditions.	350

11	DBE Program	Strategic & Regulatory	Assurance	Review controls after DBE program updates are implemented.	240
12	Watco Freight Revenue - build model to estimate monthly freight revenue	Advisory	UT Audit Interns	Build model to recalculate Freight Revenue and compare to Watco monthly reporting file.	200
13	Endpoint Management (Patching with SCCM) Computers -	IT Assurance	UT Audit Interns	UT Audit Interns to review SCCM patching reports, perform physical inventories, etc..	220
14	Analysis of Incident Reporting in OrbCAD system	Advisory	UT Audit Interns	UT Audit Interns to perform analysis of OrbCAD incident reports and possible correlation with other systems (e.g. CCR, Smart Drive, etc.)	200
15	Annual Cybersecurity Review	IT Assurance	Assurance	Annual Cybersecurity Assessment with outsourced IT Penetration & Vulnerability Assessment	240
16	Rail Systems Security (Railcomm, PTC, Signaling, etc.)	IT Assurance	Assurance	A holistic review system resiliency with a focus on key rail applications and the interdependency.	300
17	NIST Cybersecurity Framework (Facilitated Self Assessment)	IT Advisory	Continuous Improvement & QC	Internal Audit will help facilitate a self-assessment of maturity level against Cybersecurity Framework. Key controls will be documented and action plans will be developed for deficiencies.	240

18	Community Engagement & Professional Organization Support	Strategic	Continuous Improvement & QC	Internal special projects including support of local and industry professional associations (ISACA, IIA, APTA, ALGA, Toastmaster, etc.), responding to professional exposure drafts, internal training and other internal quality improvement opportunities as needed. UT Audit Intern Program (Fall & Spring).	240
19	Management Requests, Consulting & Special Projects 1) Advisor on various Committees; 2) Investigations; 3) Emerging Risks & Special Projects as requested, etc..	Multiple	Advisory / Consulting	Internal auditing best practices include allocating an undesignated contingency for management requests and other unanticipated special projects.	600
				TOTAL ESTIMATED HOURS	***5,130***

TABLE 2 – FY20 Contingency Audit Projects (To Be Used as Backups)

	Audit Project	**Risk Area**	**Audit Type**	**Audit Objective & Scope**	**Estimated Hours**
1	FTA - Passenger Transportation Agency Safety Plan program	Safety & Regulatory	Assurance	Assessing compliance with 49 CFR Part 673 - Public Transportation Agency Safety Plan (PTASP)	300
2	Fuel Controls & Hedging	Financial	Assurance	Review controls over the purchasing and hedging of fuels.	240

3	Cyber Ransomware Threats - Table Top Exercise	Technology	IT Advisory	Ransomware mock exercise facilitated by DHS/FBI.	200
4	Healthcare & Other Insurance Benefits - TPA Payments	Financial & Human Capital	Assurance	Assessing the Effectiveness and Efficiency of Management Processes to Prevent and Detect insurance overpayments/fraud. TPA (Third Party Administrator)	240
5	Facilities Maintenance & Change Over	Quality Control & Assurance	Assurance	Quality control and contract compliance with Facility Maintenance service providers.	300
6	Bridge Inspection Reports	Quality Control & Assurance	Assurance	Review year over year Bridge Inspection Reports from external engineers and ensure actions are taken.	150
					1,430