METRO | MEMORANDUM

To: Terry Mitchell, Chair, Finance, Audit & Administrative (FAA) Committee
Wade Cooper, Member, FAA Committee
Troy Hill, 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 14, 2020

Subject: **Approved FY2021 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 FY2021.

FY2021 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 FY21 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 FY21 Plan has a stronger focus on the periodically required regulatory audits (e.g. Quadrennial, FTA Triennial, QAR). Additional areas of focus are IT security, Project Connect, and financial controls. The proposed plan includes three IT projects which includes 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 Transit Store. Other projects to highlight from the FY21 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 FY21 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 FY21 Audit Plan will use a combination of internal and external resources to perform the projects. Historically the Internal Audit Department has completed approximately seven audit projects per year. The FY21 plan includes eleven assurance projects, four QC and compliance, and one advisory project, 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 which started in 2018. This Fall semester we will have ten 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 fifth 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 FY2021 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 FY21 Audit Plan.

TABLE 1 – FY2021 Audit Assurance & Advisory Projects

	Audit Project	**Risk Area**	**Audit Type**	**Audit Objective & Scope**	**Estimated Hours**
1	Semiannual Implementation Status Updates - November 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
2	Semiannual Implementation Status Updates - May 2021	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	FY2021 Risk Assessment & FY2022 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	*400*

5	FTA Triennial Review	Strategic & Regulatory	Continuous Improvement & QC	FTA Mandated	*300*
6	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 normally due by October 31, 2020, has been postponed by GAO/ ALGA due to COVID-19.	*260*
7	SOX Like Key Financial Control Testing (Transit Store)	Financial	Assurance	We will ask CFO and Controller for their suggestions on areas to review.	240
8	Project Connect - System Controls & Processes (e-Builder)	Strategic & Technology	Advisory	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
9	PTC (Positive Train Control) - Expenditures & Drawings - Contract Close-out	Strategic & Regulatory	Assurance	Review billings and support for compliance with contract terms and conditions.	350

10	DBE Program	Strategic & Regulatory	Assurance	Review controls after DBE program updates are implemented.	240
11	Annual Cybersecurity Review	IT Assurance	Assurance	Annual Cybersecurity Assessment with outsourced IT Penetration & Vulnerability Assessment	240
12	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
13	Saltillo Development Project	Operations	Assurance	Review Saltillo contracts and test compliance including revenue sharing agreements.	200
14	Petty Cash	Financial	Assurance	Periodic audit of Petty Cash as required by policy FIN-102.	160
15	Payroll Process - SOX Review	Financial	Assurance	Review payroll controls to ensure payments are timely, accurate and properly approved.	200
16	NIST Cybersecurity Framework (Facilitated Self Assessment)	IT Assurance	Assurance	Review compliance with the 108 recommended controls covering best practices, standards and guidelines designed to better manage and reduce cybersecurity risks.	200

17	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
18	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	***4,870***

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

	Audit Project	**Risk Area**	**Audit Type**	**Audit Objective & Scope**	**Estimated Hours**
1	Downtown Station - Closeout	Quality Control & Assurance	Assurance	Review contract compliance related to deliverables and payments, including final payments and related close-outs.	300
2	Project Connect - Marketing & Planning Expenditures	Strategic & Regulatory	Assurance	Review Media Plan and related contracts, audit invoices to ensure contract and regulatory compliance.	240
3	Infor System - post go live review	Strategic, Operations, IT Assurance	Advisory	Ensure the completeness and accuracy of the data that has been loaded from Spear, and review the capabilities and implementation of the system	300
4	Discounted Pass Program	Financial	Assurance	Review the internal controls related to the Discounted Pass Program.	240
5	Facilities Maintenance - Contract Monitoring & Compliance	Quality Control & Assurance	Assurance	Quality control and contract compliance with Facility Maintenance service providers.	300

6	Paratransit & Demand Response Operations	Operations	Assurance	Review billings and support for compliance with contract terms and conditions.	240
7	Board Policies/Goals - Monitoring & Reporting (e.g. OTP; Fare Recovery; DBE; Title 6 Equity Analysis; etc.)	Governance	Assurance	Review Board policies/goals to ensure that they are periodically reviewed and updated, and that related performance metrics are being tracked and reported.	200
				TOTAL ESTIMATED HOURS	***1,820***