METRO | MEMORANDUM

To: Terry Mitchell, Chair, Finance, Audit & Administrative (FAA) Committee
Wade Cooper, Member, FAA Committee
Becki Ross, Member, FAA Committee
Leslie Pool, Member, FAA Committee

CC: Randy Clarke, President/CEO

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

Date: October 13, 2021

Subject: **Approved FY2022 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 FY2022.

FY2022 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 FY22 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 Performance Audit, etc.), 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 FY22 Plan has a stronger focus on the periodically required regulatory audits (e.g. Quadrennial, FTA Triennial, QAR) and new system implementations (e.g. Oracle ERP; Infor Asset Management System). Additional areas of focus are IT security, safety, 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 a possible review of Microsoft Sharepoint Security. Other projects to highlight from the FY22 Plan include the support of the FTA Triennial Review, the Quality Assessment Review of the Internal Audit Department that is required every three years, and the audit of the P-Card transactions. Internal Audit believes these focus areas together with the other projects in the proposed Audit Plan will appropriately address the risks identified.

The FY22 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 FY22 Audit Plan will use a combination of internal and external resources to perform the projects. Historically the Internal Audit Department has completed approximately nine audit projects per year. The FY22 plan includes fourteen assurance/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 which started in 2018. This Fall semester we will have three graduate Accounting students from UT's #1 ranked Masters of Professional Accounting program who will be assisting on the Business Continuity (COOP Plan) advisory as part of their required Audit class. This is our seventh semester participating in this highly successful program, and we plan on continuing the UT 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), is performed by an external consulting firm and it is funded by the IT Department. We believe this mix of internal and external resources is sufficient to perform the projects listed in the FY2022 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 FY22 Audit Plan.

TABLE 1 – FY2022 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.)	200
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.)	200
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	FTA Triennial Review	Strategic & Regulatory	Assurance	FTA Mandated	325
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 normally due by October 31, 2020, has been postponed by GAO/ALGA due to COVID-19.	300

6	Saltillo Development Project & Lease Revenues	Operations	Assurance	Review Saltillo contracts and test compliance including revenue sharing agreements.	160
7	Transit Store with Ticket Focus	Financial	Assurance	The physical and accounting controls over both hardcopy and e-tickets.	160
8	NIST Cybersecurity Framework (Facilitated Self Assessment)	IT Assurance	Assurance	Check for compliance with best practices listed in the NIST Cybersecurity Framework	160
9	Business Continuity (COOP) Plan	Strategic	Advisory / Consulting	To review COOP plan against best practices and other transit agencies and help management develop a Dependency Map.	120
10	ERP (Oracle) Implementation Advisory	Financial	Advisory / Consulting	Compliance with contractual requirements as well as implementation methodology.	400
11	GRC & Contract Performance Management System Advisory	Operations	Advisory / Consulting	Serve as an advisor in the selection process of a tool that can meet the following two separate IT Capital Projects: Governance Risk & Compliance (GRC); and Contract Performance Mgt System recommended in the Quadrennial Audit Report.	450
12	P-Cards & IT Procurement	Financial	Assurance	Compliance with policies and identify currently unknown IT risks if IT was not consulted and did not perform a security review.	250
13	Public Transportation Agency Safety Plan (PTASP)	Operations	Advisory / Consulting	Compliance with regulatory requirements as well as best practices.	300

14	Annual Cybersecurity Review	IT Assurance	Assurance	Annual Cybersecurity Assessment with outsourced IT Penetration & Vulnerability Assessment	240
15	Benchmarking Policies & Procedures (Structure, Content, Governance & Training)	Strategic, Operations, IT Assurance	Advisory / Consulting	Benchmark CapMetro Policies/Procedures against other transit agencies and best practices in regards to structure, content, governance and training.	250
16	Support to Transit Industry & Professional Organization	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
17	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	***4,655***
	Project started in FY2021 UT Intern projects Fall 2021				

TABLE 2 – FY22 Contingency Audit Projects (To Be Used as Backups)

	Audit Project	Risk Area	Audit Type	Audit Objective & Scope	Estimated Hours
1	Infor System - post go live review	Strategic, Operations, IT Assurance	Assurance	Review internal controls and functionality of the new Infor enterprise asset management system.	250
2	Salary Adjustment & Merit Process	Strategic, Operations, Financial	Assurance & Advisory	Review the process and controls applied to implement the recommendations from Gallagher consulting.	200
3	Facilities Maintenance - Contract Monitoring & Compliance	Quality Control & Assurance	Assurance	Quality control and contract compliance with Facility Maintenance service providers.	300
4	Paratransit & Demand Response Operations	Operations	Assurance	Review billings and support for compliance with contract terms and conditions.	240
5	United Healthcare & Other Self-Insured Benefits (TPA Payments)	Financial & Human Capital	Assurance	Assessing the Effectiveness and Efficiency of Management Processes to Prevent and Detect insurance overpayments/fraud. Review self-insured TPA (Third Party Administrator) payments.	240

6	Bytemark - Account-Based System	Strategic, Operations, IT Assurance	Assurance	Bytemark system being updated to include customer account based info which increases privacy risks.	240
7	Microsoft Sharepoint & Active Directory	IT Assurance	Assurance	The confidentiality, integrity and availability of the Microsoft Active Directory and Sharepoint.	200
8	Safety Management System (SMS) - Management of Change	Operations	Advisory / Consulting	Compliance with FTA requirements related to safety and "management of change".	400
9	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 tracked and reported.	200
				TOTAL ESTIMATED HOURS	***2,270***