



To: Matt Harriss, Member, Chair, Finance, Audit & Administrative (FAA) Committee
Dianne Bangle, Member, Vice Chair, FAA Committee
Leslie Pool, Member, FAA Committee
Becki Ross, Member, FAA Committee

CC: Dottie Watkins, President/CEO

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

Date: October 11, 2023

Subject: **Proposed FY2024 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 FY2024.

FY2024 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 FY2024 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, 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.

This year's Risk Assessment (Table 3) identified the top 17 risks facing CapMetro in FY2024 and 7 of these risks are new. Some of the more significant new risks are related to the expected payroll "pass through charges" in the new Bus Operations & Maintenance contracts which will require new internal controls and processes. Additionally, the forecasted large increase in

capital projects, including the electric bus program, establishing new transit facilities and offices, MetroRapid delivery, and the standup of the new North Base Demand Response and CapMetro Police Department facilities. A notable change is the reduction of CapMetro's risks related to Project Connect because the new Joint Powers Agreement has assigned full responsibility for Light Rail FTA grant monies to Austin Transit Partnership. Some key drivers of higher risks noted are as follows: FY2024 CapMetro growth with \$411 million in projected Capital Projects and \$427 million in Operating Expenses; multiple large capital projects (e.g., McKalla Station; new Fifth & Tillery headquarters; etc.), CapMetro and service provider personnel vacancies; tight labor market with higher employee turnover and high uncertainty in the economy. Some of the service provider risk is mitigated through the planned implementation of an enterprise governance, risk and compliance (GRC) system and Internal Audit is serving as an advisor and is the lead facilitator on the GRC implementation to help ensure that controls are adequate and process improvement efficiencies are gained. Additionally, the FastPath system has been chosen by management to analyze segregation of duties in the new Oracle system and the Internal Audit Department will help management in the evaluation of SOD across Oracle (e.g., Payroll; Accounts Payable; Accounting; etc.).

One of the most impactful IT projects which will assist with the service provider oversight and management is the implementation of the Governance Risk & Compliance (GRC) systems. This project was spawned from the Texas statute required Quadrennial Performance Management review and recommendation in January 2021 that CapMetro implement a "contract management system" to help on monitoring vendor performance/compliance in Bus, Rail and Demand Response contracts. The proposed FY2024 has multiple GRC related projects with Internal Audit playing a critical role in ensuring the GRC implementation goes smoothly across various departments with internal control improvements and efficiencies being gained. Note, the development of the automation of Bus incident/accident reporting process was completed during FY2023 but the implementation was postponed due to the Bus vendor selection process and upcoming change in Bus operations/maintenance vendors from MV Transportation to Keolis effective 1/1/2024.

The FY2024 Plan also includes a focus on IT security, safety, and financial controls. The proposed plan includes three IT projects which includes a follow-up cybersecurity assessment conducted by CISA, the Annual Cybersecurity Review (i.e., IT Penetration and Vulnerability Assessments), and a possible review of Microsoft SharePoint Security. Other projects to highlight from the FY2024 Plan include the review of the ATP/CapMetro billing processes, and the new operating model in the Keolis contracted bus operations and maintenance services. Internal Audit believes these focus areas together with the other projects in the proposed Audit Plan will appropriately address the risks identified.

The FY2024 audit plan also includes a list of contingent projects (Table 2 – seven projects listed as Contingent Audit Projects) 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 FY24 Audit Plan will use a combination of internal and external resources to perform the projects. This past year the Internal Audit Department completed seventeen audit projects. The FY24 plan includes twenty-two 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 five full time auditors, and we continue to mature the UT Audit Intern program which started in 2018. This Fall semester we will have five graduate Accounting students from UT's #1 ranked Masters of Professional Accounting program who will be assisting on four advisory projects as part of their required Auditing class. This is our eleventh 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 volunteer project time for the semester as part of their Auditing class at UT. Additionally, on the IT security side we have signed up with CISA to follow-up on this years cybersecurity assessments, and 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 FY2024 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 FY2024 Audit Plan.

TABLE 1 – FY2024 Audit Assurance & Advisory Projects

	Audit Project	Audit Type	Audit Objective & Scope	Estimated Hours
1	Semiannual Implementation Status Updates - November 2023	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 2024	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	FY2024 Risk Assessment & FY2025 Audit Plan Development	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.	350
4	CapMetro/ATP Billing Processes	Advisory & Consulting	Review processes and controls to facilitate billings between ATP and CapMetro to ensure the process is properly designed and efficient.	240
5	Keolis Payroll Pass Through Controls - New Contract in Bus	Assurance & Advisory	Ensure controls are appropriate to validate the Keolis employees are paid in compliance with the Collective Bargaining Agreement and CapMetro is properly billed.	500
6	Hexagon (Infor) System - post go live review	Assurance	Review internal controls and functionality of the new Infor enterprise asset management system.	250
7	Paratransit & Demand Response Operations	Assurance	Review MTM billings and support for compliance with contract terms and conditions.	160

8	FastPath - Analyze Oracle segregation of duties	Advisory / Consulting	FastPath software has been purchased to analyze segregation of duties (SOD) across the financial transactions (e.g. Payments; Payroll; etc.)	300
9	MV Contract - Payroll Pass Through Charges	Assurance & Advisory	Ensure controls are appropriate to validate that MV employees are paid in compliance with the Collective Bargaining Agreement and CapMetro is properly billed.	160
10	Miscellaneous Revenue Controls	Assurance	Review the design and operating effectiveness of internal controls to ensure the completeness and accuracy of miscellaneous revenue.	350
11	GHG & Carbon Footprint Reporting	Advisory	Ensure environmental reporting is in compliance with the Climate Registry.	160
12	Sales Taxes - Revenue Controls	Advisory	Review controls to ensure the monthly Texas Comptroller payments are being made timely and accurately.	160
13	Investment Income - Revenue Controls	Advisory	Review controls to ensure CapMetro cash and related investments are in compliance with the Investment Policy and errors and irregularities would be prevented and/or detected timely.	160
14	Watco Freight Revenue - Revenue Controls	Advisory	Review payment controls to ensure that Watco freight revenue sharing is in compliance with contract terms.	160
15	GRC - automate Incidents/Accidents Reporting (Bus, Rail, DR)	Advisory / Consulting	Help management design and implement the automation of incident/accident reporting across Bus/Rail/DR using the GRC system.	400
16	GRC - Contract Performance Management System Advisory (Bus, Rail, DR) - Quadrennial Performance Audit recommendations	Advisory / Consulting	The Quadrennial Performance Audit Report dated 1/2021 requires that a Contract Management System be implemented. Serve as an advisor on the GRC implementation in the following areas: Contract Performance Mgt System for Bus, Rail and Demand Response.	800

17	GRC (Governance Risk & Compliance) System Implementation (Risk Register; Safety Dept; Internal Audit Dept; etc.)	Advisory / Consulting	Assist with the enterprise level implementation of the Diligent GRC system which provides the tools to automate monitoring and reporting as follows: Contract Compliance & Billings; Safety; Risk Registers; Enterprise Risk Management; Internal Audit and other departments etc..	600
18	Safety Management System (SMS) - Management of Change	Advisory / Consulting	Compliance with FTA requirements related to safety and "management of change".	400
19	Bus Charging Infrastructure & EV Program	Advisory / Consulting	Review project plans related to the EV Bus Program and evaluate where policies/procedures will need to be defined to properly support the EV fleet.	400
20	AMP Cards & New Fare Structure	Assurance & Advisory	Review process and technology controls to ensure the new AMP Card and fare structure rolls out smoothly with appropriate internal controls	400
21	United Healthcare & Other Self-Insured Benefits (TPA Payments)	Assurance	Assessing the Effectiveness and Efficiency of Management Processes to Prevent and Detect insurance overpayments/fraud. Review self-insured TPA (Third Party Administrator) payments.	300
22	McKalla Station - Design Build Effectiveness	Assurance	Review the procurement and construction process for compliance with contracts, policies, procedures and regulatory requirements.	350
23	NIST Cybersecurity Framework (CISA Facilitated Self Assessment) - re-assessment from 2023 baseline	Assurance	Check for compliance with best practices listed in the NIST Cybersecurity Framework	300

24	Annual Cybersecurity Review (Mandiant)	Assurance	Annual Cybersecurity Assessment with outsourced IT Penetration & Vulnerability Assessment	200
25	Quadrennial Performance Audit - Selection Process but FY25 Budget/Execution	Advisory		100
26	Support to Transit Industry & Professional Organization	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
27	Management Requests, Consulting & Special Projects 1) Advisor on various Committees; 2) Investigations; 3) Emerging Risks & Special Projects as requested, etc..	Advisory / Consulting	Internal auditing best practices include allocating an undesignated contingency for management requests and other unanticipated special projects.	600
TOTAL ESTIMATED HOURS				8,440

Project started in FY2023

UT Intern projects Fall 2023

TABLE 2 – FY2024 Contingency Audit Projects (To Be Used as Backups)

	Audit Project	Audit Type	Audit Objective & Scope	Estimated Hours
1	Microsoft Sharepoint & Active Directory	Assurance	The confidentiality, integrity and availability of the Microsoft Active Directory and Sharepoint.	250
2	Salary Adjustment & Merit Process	Assurance & Advisory	Review the process and controls applied to implement the recommendations from Gallagher consulting.	200
3	Rail-FRA PTC Change Management Requirements (Herzog)	Advisory / Consulting	Review compliance with the FRA's change management record keeping required for all system components and records.	300
4	Board Policies/Goals - Monitoring & Reporting (e.g., OTP; Fare Recovery; DBE; Title 6 Equity Analysis; etc.)	Assurance	Review Board policies/goals to ensure that they are periodically reviewed and updated, and that related performance metrics are tracked and reported.	300
5	Capital Project Controls (McKalla Station; MetroRapid; DR N Facility Build;)	Assurance & Advisory	Review controls related to Capital Projects, and ensure compliance with contracts in regards to deliverables and payments.	350
6	Spare Labs.com - Demand Response System Implementation	Advisory / Consulting	Review requirements and design management controls and related procurement activities for compliance with policies/procedures.	250
7	Lease Vehicle Program - non-Revenue Vehicles	Assurance & Advisory	Review lease contracts, fleet utilization, and related controls to ensure contract compliance and proper asset management.	400

TOTAL ESTIMATED HOURS

2,050

TABLE 3 – FY2023 Risk Assessment Survey Results

Response	Average (A) Impact	Average (B) Likelihood	(A x B) Residual Risk	(D) Mitigating Controls	Accept Risk	Requires Plan	"Requires Plan" Recommendations to Improve Risk Management Activities
1 Project Connect, CapMetro Delivered - Scope / Schedule / Cost	6.13	6.75	41.3	Updated JPA in June 2023 provides clarity in roles, and ATP is the primary grant recipient for LRT under the JPA. CapMetro will continue to support PMP processes, FTA requirements, and safety certifications in the role as the future Operator in the system startup. <u>Metro Rapid Delivery</u> - 1) CapMetro monthly Metro Rapid project team meeting; 2) Tri-Party meeting of appropriate department leaders (CA, ATP, COA); 3) Monthly Executive Tri-party meeting (CA, ATP, COA); 4) FTA monthly/quarterly meeting with CapMetro.	1	5	Continue to implement FTA Requirements; Coordination & Alignment with City Council; Integration with new EPPM System; Ensure that proper resources for operations and maintenance costs are available annually, mid-life and end of life to support MetroRapid, MetroRail and Light Rail projects. Ensure Project Connect agreements with CapMetro receives the following transfers as the future Operator: contracts; warranties; real estate and easements; and third party agreements. <u>MetroRapid Delivery</u> - The first two MetroRapid projects as part of Project Connect will be operationalized in 2025, so FY24 is "go-time" focused on time and budget delivery. Our organizational focus on successful delivery of these two projects should be one of our top priorities.
2 Standup of CapMetro Police Department	6.38	6.13	39.0	Chief of Police has been hired and separate Police building has been procured and is being customized for CapMetro's PD needs. Development of Policies for the certification process. An ILA has been established with GATRRS and the City of Austin. Senior staff has been hired. We regularly meet with Public Safety Committee which is appointed by the Board. Prepare to plan and train Public Dispatchers. RFP process to identify RMS system and interface with COA CAD system (CTECC). When appropriate execute recruitment campaign and efforts to hire certified and non-certified Officers. Meet with community leaders and provide updates. Have begun procuring vehicles and some in the pipeline. Coordinating with Marketing on branding/imaging, etc., of uniforms, equipment, vehicles, etc.. P&C helping develop enhanced PD training program including customer and Operator interface.	4	2	
3 Safety of Operations	6.25	5.88	36.7	Safety Policies & Training; Ops Procedures; Ops Mgt; Safety Plans; Oversight from Mgt, Fed, State & Contractors; Accountability & PDC's; Reg Requirements for Safety Plan; SMS in place; SMS plan in development for new FTA Requirements; Passenger Safety Initiatives	4	2	Improved driver training & mgt; Continued focus on safety systems/policies; Complete required Safety Plan; Develop System Safety Program Plan; Develop improved safety plans, procedures, protocols, policies, and training programs. Continue rollout of Battery Electric bus safety training. Ensure safety plans evolve with technology in a timely manner.
4 Service Provider Performance & Contract Management	5.88	6.13	36.0	Contract and oversight which includes PDC's; Employee engagement; QA in contracts & periodic audits; Contract Management Plans; Contract Monitoring Plans created by PW's; Mode-specific oversight in place; Software (GRC & Contract Performance Mgt) is in the works to help manage this.	3	3	Fine-tune what CapMetro can impact and what contractors should control; Improve and automate Bus/Rail/DR incident/accident reporting to improve timeliness and accuracy. Continue to clarify the roles and responsibilities of both MW/Keolis and CapMetro with CapMetro's responsible for the day to day service delivery and MW responsible for employee management and safety incident and accident reporting. Roles have been established with an immediate focus on the delivery of service. Over the next year, those roles need to be codified in writing. Development of scope for new management contract model with defined Performance and disincentives based on refined contractor responsibilities. Train and refine duties of existing Q/A and management staffing. Fine Tune recruiting strategy to include an industry hard look at work environment. Utilize the third party to survey employees and assist in developing a plan to attract and retain Operators and Mechanics; CapMetro leadership is developing a joint plan with MW/Keolis to address performance issues; Training program to develop and improve access skill levels of incumbent employees. A Governance Risk & Compliance software is being deployed to help with contract monitoring.
5 Electric Buses - Strategy/Delivery/Mgt	5.13	6.75	34.6	Bus Infrastructure has been scheduled and has been shared with the FTA for MetroRapid (Expo & Pleasant Valley). 2010 Plan developed with Proterra. Contingency is being developed around Proterra recent Bankruptcy. Planning for N Ops expansion with solar grid and bus charging is underway. Close coordination with Austin Energy. FTA required Fleet Transition Plan which is routinely updated. David Carr, Dir of Zero Emission Vehicles. Good contract and OEM management with the bus builders to prevent defects. Additional Field Service Techs have been added to contracts to ensure availability/reliability. New EV specialty shop to address diagnostics and repairs and related training.	3	3	Develop a Fleet Diversification Plan with changes in bus electrification field, alternative fuels (e.g. Hydrogen, etc.) with our carbon neutrality goal in mind. Continued vigilance around managing the Proterra bankruptcy risks through direct negotiations and industry channels.
6 Workforce Shortage, Competition & Development	6.00	5.75	34.5	Tool developed by BCG for workforce planning. Increases in starting pay for frontline bus and maintenance employees. Resources to supplement talent acquisition staff: executive recruiter, professional and frontline staff recruitment contract, one dedicated company to fulfill temporary employee needs. Partnership with marketing team to develop and deploy aggressive marketing campaigns. Innovative hiring incentives including increased hiring bonuses, referral bonuses, relocation and temporary housing.	2	4	Build a short and long range workforce strategy plan. Identify and create partnerships and talent pipelines.
7 ATP/CapMetro - Alignment & Business Process Optimization	5.50	5.63	30.9	JPA and amendments and ILA's will help manage this risk. The CapMetro/ATP billing process has been added to 2024 Audit Plan. Support service agreements (e.g. benefits, systems, etc.) is being updated.	3	3	Long range risk to success of program but largely out of the CapMetro sphere of control.
8 IT Risks & Cybersecurity	6.00	5.00	30.0	IT Policies/Procedures; Internal/External Audits; Ongoing training for employees; Position allocated to address Cyber Security; Monthly IT Security Review Meeting; In 2023 OSA performed benchmarking IT Risk assessment establishing a baseline and in 2024 same study will be performed to gauge progress.	3	3	Cyber Security Program; Develop Plan for external threats (virus, ransomware, etc); Ensure Cybersecurity and IT have the right resources, necessary experience level, established standards and guidelines, and procedures to properly engage in software implementations and increased technological solutions that will be forthcoming at CapMetro in an exponential way.
9 Enterprise Systems (Oracle, Hexagon, etc.) Business Process Optimization	5.88	5.00	29.4	Oracle has Executive Steering Committee that meets monthly to discuss open items and prioritize. FTA grants and requirements will drive needed new reporting. EDAP and ability to pull data quickly and routinely. EAM Consultant being hired to evaluate Hexagon asset management strategy and execution. Oracle University library is being established to track and record specialty classes completed.	3	3	Additional resources to resolve and root cause fix current EAM issues. Will establish timely training and refreshers on major systems.
10 Projected Costs vs Revenues	5.50	5.00	27.5	Annual Budgets by Department approved by mgt and Board. Monthly tracking of Actual vs Budget with reporting to Mgt/Board. Budget Dept that is separate from Actual accounting that works on ST/ALT forecasts and challenges mgt on assumptions. All material expenditures and commitments require approval from the Board. FY24 there is a freeze on FTE growth, with focus on filling/adjusting vacancies first. Developing structured process for evaluating/filling vacancies.	3	3	Strengthen project review processes and procedures to avoid scope creep. In light of ATP being the FTA direct recipient of new starts grants and light rail delivery, a thorough and critical review of workforce needs and FTE growth is needed. Some level of benchmarking with our peer systems would be beneficial with a nuanced review of our core and support functions. Previous precipitous growth in certain departments leading up and immediate post referendum should be re-evaluated in light of the revised JPA and division of responsibilities.
11 Establishing Transit Facilities & Offices	5.00	5.50	27.5	Facility Catalogue is being developed to support the Facility Master Plan. SOG in Hexagon and required NTD reporting. Facilities costs is included in the long range financial plan.	3	3	A centralized and coordinated Facility Management Plan needs to be put in place.
12 Political Risks (Federal & State)	4.88	5.38	26.2	The full Gov't Affairs team is focused on political risks and ensuring emerging risks are identified, monitored and addressed. Lobbyist help to support our 4 FTE's and workshop to optimize coordination will occur. Coordinated voice on Project Connect matters between ATP/CapMetro is high focus area.	4	2	Largely out of CapMetro sphere of control.
13 Employee Retention & Succession Planning	5.00	4.88	24.4	FTI Bus Operator retention study. Development of leadership training plan. Employee Engagement Survey. Competitive merit increase budgeted for FY 23. Frontline employee pay in fixed route increased to be more competitive.	2	4	Succession Planning / High Potential <ul style="list-style-type: none"> Identify critical capabilities to develop in future leaders Create strategy-aligned criteria to identify future leaders Provide future leaders with targeted development/Leadership Development Define leadership expectations Access Leadership Development Needs Define a leadership development strategy
14 Ridership Levels & Creating a Culture of Ridership	5.13	4.38	22.4	Identify new core ridership segments and review dormant commuter market, establish new baseline for bus, Rapid, rail, event, pickup and review with FY 2023 budget to develop recommendations on how best to market and incentivize while also leveraging the new fare program to attract more riders.	3	3	Balance between transit dependent and transit riders of choice in our Service Plan and reflect that in our fare strategy. Marketing strategy targeting commuters and appealing to the low price of transit as compared to car ownership; sustainable plan for the unhouse and non-destination rides, re-open dialogue with employers. Development of long-term strategy for Pickup service. Develop the new baseline for bus service (local and commuter) based on changes within the work space that have become the new normal. A clear understanding of what service levels we are offering based on service demands.
15 Recession &/or Inflation	5.25	4.00	21.0	Sales tax budgeting is conservative.	5	1	Salary review for all employees will occur to ensure competitive with market.
16 Staffing & Visibility/Utilization Across Departments	4.38	4.63	20.2	Process for requesting and approving additional staffing or other resources during annual budget process	4	2	Improving workforce planning tools and support for department to identify both ST and LT staffing plans; The Strategic Plan will help address this. Dashboards for each department on Central. Develop communications plan.
17 Strategic Focus vs Fast Growing Priority Lists (ST vs LT)	3.63	5.38	19.5	Development of updated strategic plan, KPIs being developed to measure Actions from updated Strategic Plan. Plan will be updated for FY24. SET established priorities for FY23 from Strategic Plan and will cascade actions.	3	3	Opportunity for better planning and systematic approaches; plans still in development but required; Need to do more as it relates to adoption and cascading strategic priorities down through the organization. Leadership will be facilitating a long range plan exercise for the future state of CapMetro. The current Strategic Plan will become an annual work plan to support it along with setting annual agency priorities.
Severity of Impact (Rating of 0 to 9)		Likelihood of Occurrence (Rating of 0 to 9)		Here are the standard definitions of the two concepts:			
Minor/Green = 0 to 3		Remote/Green = 0 to 3		Inherent risk represents the amount of risk that exists in the absence of controls.			
Moderate/Amber = 3.1 to 6		Possible/Amber = 3.1 to 6		Residual risk is the amount of risk that remains after controls are accounted for.			
Critical/Red = 6.1 to 9		Likely/Red = 6.1 to 9					