Audit Committee

September 19, 2025 City Hall Building – Uptown Conference Room – 1st Floor
11:00 AM 1111 1st Avenue, Columbus, GA 31901

Members: Vice Chair Councilor Toyia Tucker, Mike Baker, Tyson Begly, Mike Bruder and Councilor Glenn Davis

Recording Secretary: Clerk of Council Lindsey G. McLemore

CCG Staff: Deputy City Manager Pam Hodge *(via teleconference),* Mayor Skip Henderson *(via teleconference; joined at 11:43 a.m.)*

Mauldin & Jenkins Representatives: Director Craig Carter, Information System Auditor Ben Barendse *(via teleconference),* Government Advisory Consultant Austin Hickox *(via teleconference),* and Director Jon Hightown *(via teleconference)*

Call to Order

A regular meeting of the Audit Committee was called to order by Councilor Toyia Tucker, Vice Chair, at 11:12 a.m.

ORDER OF BUSINESS

I. Minutes

Approval of minutes for July 7, 2025, Audit Committee Meeting. *(NOTE: Committee called for the update. Minutes were not addressed and no vote was taken.)*

II. Update – Mauldin & Jenkins

Craig Carter, Director, Mauldin & Jenkins, provided a draft presentation *(2025 IA Risk Assessment & Annual Audit Plan)* agenda listing key topics for discussion; (A) Executive Summary, (B) Project Approach, (C) Risk Assessment Results, (D) Developing the Annual Plan, (E) Next Steps, and (F) Risk Based Internal Audit Approach – Appendix A.

A. Executive Summary

The risk assessment was completed through 15 interviews and review of 87 government documents, defining the Risk Universe as of June 30, 2025, and establishing the Audit Universe with 90 rated entities.

A nine-category risk taxonomy was developed, producing a Risk Register of 630 unique risks, with departments assessed for inherent risk (likelihood, impact, and fraud risk).

Results identified six critical-risk and 32 high-risk departments/offices and highlighted the top 30 risks based on City Council minutes from the past 12 months; observations and recommendations were included in the draft report.

Tools and processes were established to support the Annual Internal Audit Plan, annual risk updates, and implementation of a risk-based internal audit approach.

B. Project Approach

The Risk Assessment identified, assessed, and prioritized the Government's strategic, financial, operational, and legal/regulatory risks to support development of a risk-based Annual Audit Plan.

The project included initiation and planning (kickoff with stakeholders, interview scheduling, and development of an information request list).

Information was gathered through management interviews and review of documentation related to strategic initiatives, financial performance, staffing, operations, and citizen concerns.

Fieldwork and analysis involved reviewing interview and document results and scoring auditable units based on likelihood and impact to identify higher-risk entities and potential audit activities.

The process concluded with validation and reporting, including sharing preliminary observations, gathering stakeholder feedback, conducting additional analysis as needed, and preparing the final report for presentation.

C. Risk Assessment Results

<u>Major Changes</u>

Several key changes were identified as significant risk drivers affecting governance, operations, financial stability, workforce capacity, and service delivery.

- Organizational changes
- Turnover in leadership
- Ongoing financial investigations
- Workforce retirements
- Challenges in recruiting and retaining qualified staff
- Shifts in organizational culture
- Federal funding priorities
- Increase in large capital projects
- Operational challenges related to fleet maintenance and solid waste collection

    - Procedural and control changes
    - Cybersecurity
    - Legal settlements related to public safety

Risk Taxonomy & Risk Register

A Risk Taxonomy was developed grouping risks into nine categories to better organize risks impacting the government and to establish a risk “library.”

Barriers to Meeting Goals & Objectives

Barriers were identified as impacting the Government’s ability to achieve objectives and strategic initiatives, with the intent to identify key impediments and primary drivers.

- Most frequently cited challenges included:
    1. Staffing constraints
    2. Limited skills/knowledge/experience/training
    3. Financial constraints
    4. State and federal regulations
    5. Securing alternative funding sources
    6. Infrastructure maintenance needs
    7. Recruiting challenges (access to experienced, certified resources such as heavy equipment operators and mechanics)
    8. Employee retention and satisfaction
    9. Interdepartmental collaboration
    10. Resistance to change

Common Themes & Interdependencies

A review of major risk themes and evaluated interdependencies to better understand how risks impact one another across the organization.

The objective included identifying and documenting emerging risks and new concerns influenced by market dynamics and evaluating alignment with the Government’s strategy and plans.

Thirteen (13) areas were identified as persistent challenges, along with the emerging threats these challenges may pose to achieving organizational goals and objectives.

Critical & High Risks

Critical and high risks were identified and rated using the following scale:

- Low: Scores 1–4
- Medium: Scores 5–6
- High: Scores 7–9
- Critical: Scores 10 or higher

Thirteen (13) departments/offices were rated as critical and/or high-risk entities.

FOLLOW-UP:

- Recommend a third-party cybersecurity audit for the IT Department. *(Councilor Tucker, Vice Chair)*

Observations & Recommendations

Recent organizational changes highlight the need to strengthen decision-making and oversight to rebuild public trust and improve transparency and accountability.

Recommended establishing a sustainable Governance, Risk, and Control (GRC) framework to assess internal control maturity, guide improvements, evidence compliance, support strategic objectives, and strengthen SOPs.

Noted that new leadership creates an opportunity to reset organizational direction, recommended reinforcing tone at the top across the organization.

Recommended the repositioning Internal Audit by revising the IA Charter to clarify authority and access, implementing a risk-based audit approach, reducing forensic emphasis, and documenting processes consistent with IIA standards.

Recommended strengthening Audit Committee governance by formalizing procedures, expanding the AC Charter, establishing executive session protocols per Georgia OMA/ORA, providing governance/internal control and GRC training, and conducting annual self-assessments.

Recommended improving department-level process maturity through Process Analysis/Business Process Optimization to support continuous improvement and address staffing and funding challenges.

Recommended establishing IT governance and oversight through an IT Steering Committee to create technology standards, ensure IT involvement in technology purchases/projects, monitor compliance and key metrics, and assess staffing/consulting needs.

Identified cybersecurity capacity and tooling gaps (24/7 monitoring and lack of SIEM); recommended evaluating service models, conducting penetration testing within one year, and completing a NIST 800-53 audit within two years, including Business Continuity/Disaster Recovery controls.

D. Developing the Annual Audit Plan

Foundational Elements – Effective Internal Audit

Foundational elements are required for an effective Internal Audit (IA) function, noting that each element is critical and that additional enhancements should build upon strong execution of these fundamentals.

Emphasis was placed on maintaining good supporting documentation and ensuring the IA function is right-sized**,** fit for purpose, and aligned with regulatory requirements**.**

The Internal Audit Annual Cycle

It was noted that the Risk Assessment should be refreshed annually to reflect changes in the new fiscal year's Strategic Plan, Budget, and priorities**.**

A full, de novo Risk Assessment should be conducted every three to five years**.**

Internal Audit Plan Development – Internal Audit Activities by Phase

Internal Audit Cycle / Phases: (1) Audit Planning, (2) Audit Kick-off, (3) Audit Fieldwork, (4) Findings & Recommendations Development, (5) Audit Report Development & Issuance, and (6) Audit Assessment & Audit Committee Reporting.

- Phase 1 – Audit Planning (Key Activities): Form audit team; draft planning memo; send announcement memo; issue information and interview request lists; and develop a communication plan.

- Phase 2 – Audit Kick-off (Key Activities): Review client documentation; understand processes and identify risks; draft audit program; conduct entrance meeting; and update planning memo/scope as needed.

- Phase 3 – Audit Fieldwork (Key Activities): Execute audit program; hold status meetings with management; document preliminary issues and evidentiary support; and organize workpapers.

- Phase 4 – Findings & Recommendations (Key Activities): Discuss and validate preliminary issues with process/control owners; draft recommendations; and review with management.

- Phase 5 – Report Development & Issuance (Key Activities): Issue draft report; request and incorporate management responses; finalize responses; issue final report; and conduct closing meeting.

- Phase 6 – Audit Assessment & Committee Reporting (Key Activities): Conduct audit debriefs and engagement assessments; summarize results for Audit Committee reporting; and incorporate results into the Internal Audit Value Scorecard.

Audit Metrics/Timelines:

- Planning begins 4 weeks before fieldwork; announcement memo sent 3 weeks prior; information request list sent 2 weeks prior; interview request list 1 week prior.

- Planning memo and audit program completed before fieldwork; fieldwork completed within 6 weeks with weekly status updates.

- Draft report issued within 10 days of fieldwork completion; final report issued within 15 days; rewrites limited to three drafts.

- Workpaper reviews completed within 2 days; engagement assessment completed within 15 days of report issuance; issues entered tracking database and summarized for Audit Committee reporting.

E. Next Steps

Continuous Improvement

Continuous Enhancement (FY2025 and Beyond): The Committee discussed the need for ongoing monitoring, analysis, and assessment of the Government's client-facing service delivery and support processes to achieve and maintain an improved and effective control environment.

F. Risk Based Internal Audit Approach

Internal Audit Role: Internal Audit will advise stakeholders on risk and control matters based on the Government's overall risk profile, supporting continuous improvement in the control environment and contributing to a reduction in the Government's overall risk exposure over time.

Discussion & Comments:

- **Clerk of Council Lindsey G. McLemore** shared her perspective on the struggles faced particularly by the Clerk of Council's Office with no history of Standard Operating Procedures being in place and limited to no cross training. These are the same structural issues impacting many departments, and have contributed to the boards, commissions and authorities being out of compliance.
- **Committee Member Mike Bruder** shared the importance of the implementation of succession planning.
- **Vice Chair Toyia Tucker, Councilor,** suggested looking into restructuring personnel to ensure the most effective output.

Adjournment

The meeting was declared adjourned at 1:15 p.m.

Lindsey G. McLemore

Lindsey G. McLemore
Clerk of Council