GWINNETT COUNTY
DEPARTMENT OF FINANCIAL SERVICES
PURCHASING DIVISION

75 Langley Drive | Lawrenceville, GA 30046-6935
(O) 770.822.8720 | (F) 770.822.8735
www.gwinnettcounty.com

March 27, 2026

Addendum #1
RP0011-26
Provision of Information Technology and Other Internal Auditing Services on an Annual Contract

Questions & Answers:

Q1. What flexibility exists for majority remote work if it is the primary service delivery method?

A1. The service provider cannot provide all resources that are fully remote for the engagement. Remote work is not expected to be the primary service delivery method unless/until a team member's ability to perform and collaborate has been demonstrated on this engagement and Internal Audit (IA) determines remote work is in the best interest of the engagement.

Q2. The request for proposal (RFP) lists example IT control areas but does not commit to specific audit topics for the first year. What are the planned IT audit topics for the initial engagement year?

A2. The 2026 audit plan's IT audit engagements include Internal Firewalls, IT Asset Management, User Access Control, and a post-implementation review of Oracle Fusion.

Q3. The RFP states 240 applications in the portfolio. How many are considered critical or in-scope for audit purposes?

A3. Applications are scoped into the audit engagement based on risk and applicability to each audit. There are standard critical applications such as the enterprise resource planning (ERP) application, financial applications, security tools, etc.

Q4. What network segmentation exists between ITS-managed systems and departmental IT operations?

A4. Internal Audit cannot provide this or other details about County network security.

Q5. Are there Operational Technology (OT) and Industrial Control Systems (ICS) systems in scope (e.g., water, facilities management) or is the audit limited to enterprise IT?

A5. OT/ICS systems may potentially be audited but are not on the current 2026 Audit Plan. The Audit Committee approves a plan each year.

Q6. The RFP references CIS standards as the primary audit benchmark. Which CIS Implementation Group level does the County target (IG1, IG2, or IG3)?

A6. CIS Implementation Group levels are relevant in risk ranking and prioritization of controls rather than to filter controls in or out of scope based on an overall Implementation Group level target.

Q7. What is the current state of documentation for IT policies, procedures, and standards? The RFP states auditors should assume controls are not pre-documented.

A7. Auditors should assume controls are not pre-documented and that procedures and standards may or may not be comprehensive.

Q8. Are there specific regulatory audits (PCI-DSS, HIPAA, CJIS) that overlap with the IT audit plan, or are those handled separately?

A8. Regulatory audits are handled separately.

Q9. What is the expected timeline for completing each IT audit engagement (e.g., weeks per control area)?

A9. This is estimated at the beginning of each engagement during scoping. Each IT audit engagement tends to take several months.

Q10. What is the preferred reporting cadence—are interim status updates expected beyond the project management tool?

A10. Internal Audit's designated full-time, on-staff IT Audit Manager will be actively involved in the audits and work closely with any external staff, collaborating on an ongoing basis and communicating multiple times per day. As a result, IA should always be aware of project status, but IA currently holds weekly to biweekly status updates that include auditees as well.

Q11. What specific IA project management tool is in use (the RFP references an online portal and SharePoint proficiency is desired)?

A11. SharePoint is the project management tool currently in use.

Q12. Is there a target month for the first audit engagement to begin after the June 4, 2026 anticipated start date?

A12. No, this will depend on the status of audit work at that time.

Q13. How responsive are County department personnel for audit interviews and walkthroughs—are there known scheduling constraints?

A13. Personnel are generally responsive for interviews and walkthroughs. Internal Audit asks about scheduling constraints at the beginning of each engagement.

Q14. What data formats and systems will auditors need to access (e.g., Active Directory exports, firewall logs, configuration files)?

A14. It is highly unlikely that direct access to systems will be provided to external staff. External staff will submit data requests and auditees will provide extracts and documentation that varies by audit.

Q15. Will County personnel provide data extracts, or must auditors coordinate directly with ITS for data requests?

A15. With assistance, auditors must coordinate directly with ITS, working side by side with the County's designated full-time IT Audit manager.

Q16. What is the established or estimated budget for this project?

A16. There is approved funding for this project that is in line with current pricing. The County expects each service provider to propose a competitive price. Award will be made to the highest scoring service provider.

Q17. Is there an incumbent service provider or current provider for these services?

A17. Yes.

Q18. Will the County accept a proposal that is limited to the Information Technology auditing scope (Item #1, #2, and #3 on the Fee Schedule), while excluding the Non-IT Related Auditing Services (Item #4)?

A18. Yes, with the important caveat that the service provider must have internal audit experience comparable to the nature of the audit work described in the RFP. If the service provider is not experienced or knowledgeable in audit concepts, even with significant IT expertise, the service provider will be scored accordingly.

Q19. Why is the County rebidding early?

A19. The current contract is an annual contract with options to renew and can be rebid in lieu of renewing if desired by the service provider or the County.

Q20. The RFP references the County's 2026 audit plan. Can the County clarify which IT audit engagements within the plan are expected to require external staff augmentation during the first year of the contract?

A20. The 2026 audit plan's IT audit engagements include Internal Firewalls, IT Asset Management, User Access Control, and a post-implementation review of Oracle Fusion.

Q21. For engagements outside the IT audit program, can the County provide examples of the types of operational internal audits that external staff may be asked to support?

A21. Examples of engagements outside the IT audit program are available on the County website here: https://www.gwinnettcounty.com/government/departments/county-administrator/internal-audit/audit-reports

Q22. The RFP indicates that work will generally be conducted in person at County offices. Can the County provide an estimate of the expected proportion of work performed on-site, hybrid, or remote?

A22. This may vary by audit phase. For example, walkthroughs may be conducted on-site, whereas testing could potentially be performed remotely. Needs may also change. Service providers need to be able to perform work on-site when needed without compensation for travel.

Q23. The RFP notes that all workpapers will be maintained within the County's online project management portal. Can the County confirm which platform is used and whether standard audit templates will be provided?

A23. The project management portal in place at the time of this RFP is SharePoint. The audit team also uses Teams to collaborate with external staff. Standard templates will be provided for work papers. The portal and platform are Windows-based and on the County network.

Q24. The RFP indicates that external staff will not run automated scanning tools in the County's environment. Will the County provide existing vulnerability scan results, monitoring reports, or other security tool outputs to support audit testing where applicable?

A24. The RFP indicates that service providers should assume that running automated scanning tools will not be possible. Internal Audit may request scan results, monitoring reports, or other security tool outputs from the auditees when these deliverables are aligned with controls in place and audit topics.

Q25. If the County elects to award contracts to multiple service providers, how will audit assignments and hours be allocated among the selected service providers?

A25. This would depend on service provider capabilities, availability, and audit plan, which is approved annually by the Audit Committee.

Q26. Does the County maintain existing control frameworks, policies, or control inventories that external staff may leverage when developing the Risk Control Matrix (RCM)?

A26. As noted in the RFP, service providers should assume they will need to understand and document controls by working with County personnel rather than obtaining a clean listing of controls already documented for any given audit topic. The County is continuously improving and the latest documentation available may not be up to date. The RCM is developed based on a combination of industry standard controls (CIS) and understanding gained from working with control owners and executors.

Q27. The RFP indicates a preference for an in-state presence. Would the County consider service providers that can provide regular on-site staffing and travel to County facilities as needed, even if the primary office is located outside Georgia?

A27. The County would consider this if the service provider already had an in-state presence. The primary office does not need to be located in Georgia, but an existing presence is required that is not dependent on the award of this contract.

Q28. Has the County previously engaged external service providers to provide IT audit or internal audit services similar to those described in this RFP?

A28. Yes, the incumbent is an external service provider.

Q29. If applicable, can the County provide the following information related to prior engagements:

- Approximate annual hours incurred for similar services
- Approximate fees paid for those services
- Typical number of audit engagements or projects completed annually

A29. 2025 total annual hours were 1,748. The incumbent service provider billed a total of $210,000. The incumbent service provider conducted 3 engagements in 2025.

Q30. Has the County established an estimated annual budget range for the services described in this RFP?

A30. Please see A16.

Q31. The RFP states the IT audit program covers three to four control areas per year with a combined total that may exceed 70 controls. Will the Office of Internal Audit confirm which specific CIS control areas from the RFP's list of 14 are included in the 2026 audit plan, or are those domains still being finalized?

A31. The Audit Committee approves a plan each year. For 2026, the plan includes: Internal Firewalls, IT Asset Management, User Access Control, and a post-implementation review of Oracle Fusion.

Q32. The RFP estimates 1,200–1,400 total annual hours across all resources and requirements. What is the anticipated breakdown of hours by role—specifically the IT Senior Auditor versus the IT Audit Manager/Director versus the IT Staff Auditor? The RFP notes the Manager/Director is anticipated at approximately 50–150 hours.

A32. Please see Page 9 of the RFP.

Q33. The RFP references a one-year initial contract term beginning June 4, 2026, with four annual renewal options. Does IA plan to have the contract fully executed before June 4, allowing staff to begin on that date, or will the start date shift if contract execution is delayed?

A33. IA plans to have the contract fully executed, but if unexpected circumstances delay contract execution, the start date may be delayed.

Q34. The RFP states that external staff may not run automated scanning tools and that GRC software is not available. Does this prohibition apply to all audit phases including planning and risk assessment, or only to active fieldwork? Are there any County-approved data analysis tools (e.g., Excel pivot analysis, IDEA, ACL) that external staff may use during testing?

A34. The RFP states that submitting service providers should assume automated scanning tools cannot be used and that GRC software is not available, and this applies to all audit phases. Auditors frequently use Excel, including pivot analysis, and Internal Audit is open to hearing about tools available from submitting service providers if the tools do not have to be run on the County network.

Q35. If IA cancels or defers an engagement after external staff have already begun planning or fieldwork, what is the compensation model—will external staff be paid for all hours worked to date at the standard hourly rate, or is there a minimum billing floor per engagement?

A35. External staff are paid for hours worked at the standard hourly rate. There is no minimum billing floor per engagement.

Q36. The RFP states the awarded service provider is responsible for re-work or onboarding resulting from personnel turnover during an engagement. Does IA have a defined method for calculating re-work costs, or is this determined case-by-case? Is there a cap on the re-work obligation per engagement?

A36. If this were to become an issue, rework hours would be determined case-by-case without a cap.

Q37. If the scope of a particular audit engagement expands beyond the originally agreed control count or hours after fieldwork has commenced, what is IA's process for approving additional hours—does this require a formal change order, a purchase order amendment, or written email approval from the Internal Auditor?

A37. The contract will not be amended to add additional hours. If the audit engagement's work still fits within the annual not-to-exceed amount per the contract, email approval from Internal Audit would suffice. The annual not-to-exceed amount is a hard stop.

Q38. Of the 14 CIS control areas listed in the RFP—asset management, user access, malware protection, incident response, disaster recovery, administrative accounts and elevated privileges, firewalls and perimeter defenses, monitoring and logging, security architecture and design, vulnerability scanning and patch management, application security, software management, helpdesk and project portfolio management, and vendor management—which specific domains are included in the 2026 IT audit plan?

A38. For 2026, the plan includes: Internal Firewalls, IT Asset Management, User Access Control, and a post-implementation review of Oracle Fusion.

Q39. The RFP describes an ITS department of approximately 152 full-time and 20 part-time employees supporting a 240-application portfolio. Approximately how many of those 240 applications are considered Tier 1 or mission-critical, and does IA maintain a risk-ranked application inventory that external staff may reference during planning?

A39. The audit team uses a risk-based sampling approach. Information gathered in walkthroughs for the engagement will help determine the applications in scope. IA does not maintain its own risk-ranked application inventory.

Q40. Does the County currently operate a centralized SIEM, EDR, or vulnerability management platform? If so, would external staff have read-only access to view existing dashboard outputs or scan results to assist manual control testing, or is all evidence gathering limited to walkthroughs, interviews, and document review?

A40. Internal Audit cannot provide this or other security-sensitive information about controls in place. Currently, data typically is obtained through data requests or captured during observation sessions with screen-sharing.

Q41. Has IA defined which CIS Implementation Group (IG1, IG2, or IG3) it uses as its primary baseline for control assessment, and which version of the CIS Controls (v7, v7.1, or v8) is currently in effect at the County?

A41. CIS Implementation Group levels are relevant in risk ranking and prioritization of controls rather than to filter controls in or out of scope based on an overall Implementation Group level target. ITS generally **uses the most current version of CIS standards.**

Q42. Does the County's IT environment include cloud infrastructure (Azure, AWS, or GCP)? If so, are cloud-hosted systems within the IT audit program's scope, and would external staff be expected to assess cloud-specific controls such as IAM policies, storage encryption, or network segmentation?

A42. IA team will perform Scoping activities in the planning phase of any given audit will determine which cloud infrastructure is applicable to the engagement.

Q43. Is a Privileged Access Management (PAM) solution currently deployed across the County's environment? If so, which product is in use, and does the IT audit program scope include reviewing PAM configuration and access logs?

A43. Internal Audit cannot provide this or other security-sensitive information about controls in place. IT audit engagement scopes are defined upon audit initiation.

Q44. Which enterprise IT Service Management (ITSM) platform does the County use for incident and change management (e.g., ServiceNow, BMC Remedy, Cherwell)? Will external staff have access to review ticket data and change records as part of IT audit testing?

A44. IT uses TeamDynamix (TDX) as the ticketing system. External staff generally do not have access to the system. The IT Audit Division Director will assist external staff with obtaining extracts requested or tickets.

Q45. ITS works in tandem with departmental IT staff across County departments. Does the IT audit program typically audit ITS-managed systems only, or does scope extend to departmental IT staff and systems that operate independently of ITS—for example, law enforcement IT, financial systems, or court technology?

A45. The scope may extend to other departments, but the IT audit program typically focuses on ITS-managed systems.

Q46. The RFP references proficiency in SharePoint as desired. Is SharePoint the specific platform IA uses as its project management portal for audit work papers and status tracking, or does IA use a separate audit management tool (e.g., TeamMate, AuditBoard, Workiva)?

A46. Internal Audit currently uses SharePoint.

Q47. For IT audit engagements focused on application security or software management, does IA typically scope a representative risk-based sample of the 240-application portfolio, or does each engagement attempt to evaluate controls across the full portfolio?

A47. The audit team uses a risk-based sampling approach. Based on walkthrough for the engagement will determine the application in scope.

Q48. Does the County maintain an enterprise architecture diagram or network topology document that external staff can reference during the planning phase of infrastructure-related audits (firewalls, perimeter defenses, monitoring and logging)?

A48. Yes.

Q49. What is the County's current endpoint operating system environment (e.g., predominantly Windows 10/11, any macOS or Linux endpoints), and approximately how many total endpoints are managed by ITS?

A49. The County mostly uses Windows with some Linux servers. The count numbers will be provided during the planning phase for the engagement.

Q50. Does IA currently hold an external quality assessment (EQA) certification from the IIA, or is conformance self-assessed? If an EQA is planned during the contract term, would external staff be expected to contribute to preparation, and would that time fall within the 1,200–1,400 annual hour estimate?

A50. IA was peer reviewed in 2023 through ALGA and found to conform with IIA standards. Audit work is generally conducted in such a way that evidence of conformance results from day-to-day operations. External staff have not been expected to contribute to preparation for internal or external quality assessments.

Q51. Does the County operate a formal data classification policy that external staff must follow when handling audit evidence and work papers? If so, what classification levels exist, and what handling requirements apply to each level during the audit engagement?

A51. External staff usually have similar access to IA, but IA and ITS will determine if certain data is only handled by internal resources. Expectations are that external staff must save County data and audit work products in secure County storage or an agreed upon location.

Q52. The RFP states external staff must "understand and document controls by working with County personnel rather than using existing documentation or prior audits." If IA provides a prior audit report as planning context, may external staff reference it for scope understanding without using it as primary evidence for current-year testing?

A52. Yes.

Q53. The RFP requires external staff to follow IA sampling and data request standards. Will the awarded service provider receive IA's sampling standards documentation before engagement kickoff? Specifically, does IA use attribute sampling, statistical sampling, or a risk-based judgmental sampling approach for IT control testing?

A53. Yes, the awarded service provider will receive the standards. The sampling approach may vary depending on the control.

Q54. Does IA use a standard Risk Control Matrix (RCM) template that external staff must follow, or are external staff expected to build the RCM structure from scratch for each engagement? If a template exists, will it be provided to the awarded service provider before engagement kickoff?

A54. An RCM template with standard fields will be provided to external staff.

Q55. The RFP requires draft reports to be "consistent with prior IA reports in style, level of detail, and content." Will IA provide a sample redacted prior IT audit report to awarded service providers before the first engagement begins so that format, tone, and depth expectations are clearly understood?

A55. IA can provide sample IT audit reports during the planning phase of the first engagement.

Q56. The RFP prohibits the use of Artificial Intelligence in conducting audit work. Does this restriction cover AI-assisted documentation or writing tools used to format work papers and draft narratives, or is it limited to AI systems that directly analyze County systems or data?

A56. The RFP states, "Service providers should assume the use of Artificial Intelligence (AI) will not be permitted in conducting this work." External staff must disclose the nature of any AI assistance they use in the normal course of business or intend to use on County engagements for formatting or narrative drafting purposes. In work papers and reports, all statements must be supported by audit evidence or industry standards (not AI search results). Security-sensitive information is prohibited from being entered into an AI tool.

Q57. The RFP lists 14 example IT audit control areas and uses the word "examples." Are all 14 areas potentially in scope for any given year, or has IA determined that certain areas fall outside the IT audit program? Specifically, will any engagement require active vulnerability testing or penetration testing, or is the program limited to control design and effectiveness review?

A57. The program is generally limited to control design review and effectiveness testing.

Q58. The RFP requires external staff to track remediation statuses at least quarterly and validate corrective action with evidence. Does this remediation tracking work fall within the 1,200–1,400 annual hour estimate, or is it considered a separate deliverable outside those hours?

A58. This falls within the annual hour estimate.

Q59. The RFP requires external staff to provide a secure channel or virtual environment for communication with IA. Must this channel be hosted within County infrastructure, or may external staff use an independently hosted encrypted platform (e.g., Microsoft Teams or encrypted email)? Are there specific data handling or classification requirements for work papers transmitted outside the IA project management portal?

A59. Typically, the County will provide an extranet account to access SharePoint and Teams. If there is an issue with this approach, an alternative must be discussed prior to implementation. It is important for IA to have access to work papers and documentation at all times

Q60. When IA designates an additional County employee to work alongside external staff as IT Senior Auditor on a specific engagement, how is the external staff member's role expected to adapt—does the role maintain the planned scope independently, take on a supporting function, or involve redistribution of work to prevent duplication?

A60. This has not been a frequent occurrence. The assignment of internal staff would be responsive to resource or performance needs in the IT audit program, and roles could vary according to needs.

Q61. How frequently does IA expect the project management tool (SharePoint or equivalent) to be updated with control testing status summaries—daily, weekly, or at defined audit milestones? Is there a standard status reporting template that external staff must use?

A61. Frequency at minimum is weekly, but more frequent updates and answers to questions may be expected through email and Teams messages.

Q62. The RFP states external staff must work with IA to develop risk-based test plans and that IA approval is required before testing begins. What is IA's typical turnaround time for reviewing and approving submitted test plans, and how are disputes over test scope or sampling methodology resolved?

A62. The typical turnaround time is less than a week. In regard to disagreement, it is settled through final decision by Director of IA.

Q63. Is the external staff member responsible for independently scheduling walkthrough meetings with County ITS and departmental personnel, or does IA arrange those meetings through its own project management process? What is the expected lead time for scheduling access to system administrators or control owners?

A63. There are some occasions where the external staff schedule meetings. Most meetings are managed by the IT Audit Division Director. Control owners expect two weeks' lead time on average, but this varies in practice.

Q64. For IT audit engagements covering incident response and disaster recovery, does IA expect external staff to review and test actual recovery procedures (e.g., tabletop exercises, recovery time objective validation), or is the scope limited to policy and plan documentation review?

A64. The scope of evaluation would be determined during the planning phase of the audit. In general, IA evaluates management's controls and does not perform controls. As an example, IA may ask to review the results of tabletop exercises but would not conduct these exercises.

Q65. When IA assigns internal staff to revise a deliverable or work paper, does the external staff member's billing stop, continue at a reduced rate, or continue at full rate pending completion of the County's review cycle?

A65. A conversation would be required between the County and the service provider about the rework or unsatisfactory work.

Q66. The RFP references IIA Global Internal Auditing Standards (GIAS) conformance. Does IA require external staff to document their work in alignment with a specific GIAS domain (e.g., Domain IV – Managing the Internal Audit Function, Domain V – Performing the Work), and will IA provide a mapping of GIAS requirements to its internal work paper standards?

A66. External staff should be proficient in following the GIAS requirements mentioned in this question. GIAS requirements are built into most IA procedures and templates.

Q67. The RFP states potential findings should be reviewed promptly with departmental management and root causes identified. Does IA define a maximum number of business days between identifying a potential finding and conducting the management discussion, and is the external staff member expected to draft the finding write-up before or after the management meeting?

A67. Typically, a conclusion is drafted in the work paper to be discussed with the auditee. Based on feedback from the auditee, additional updates may be made before a recommendation is drafted (if applicable) for the audit report.

Q68. For control areas involving monitoring and logging or firewalls and perimeter defenses, does IA expect external staff to review actual system configurations and log samples (provided by ITS in a controlled manner), or is testing limited to interviewing ITS personnel and reviewing policy documentation?

A68. Yes, IA expects external staff to go beyond interviewing ITS personnel and reviewing policy documentation. Interviews and policy documentation would only offer insight into the design of a control and its intended operation.

Q69. How frequently does IA expect the project management tool to receive interim deliverables (e.g., completed RCMs, draft test results) versus final engagement deliverables? Is there a defined deliverable acceptance process with formal sign-off at each milestone?

A69. Frequency at a minimum is weekly, but there are times where updates can be through email and Teams messages more frequently. Milestones are discussed during planning. The IT Audit Division Director is closely involved and communicates with external staff on an ongoing basis.

Q70. The RFP does not include sample templates for the Risk Control Matrix, test plan, or audit report. Will IA provide these templates to the awarded service provider during the onboarding period, or are service providers expected to submit proposed templates for IA approval?

A70. IA will provide templates during onboarding.

Q71. Does IA require engagement-level deliverables (RCMs, test plans, work papers, draft reports) to be submitted in a specific file format (e.g., Word, Excel, PDF), and are there naming conventions or version control standards that external staff must follow within the project management portal?

A71. File format should match the format that the templates are in. Granular details such as naming conventions will be discussed after the successful service provider is onboarded.

Q72. The RFP states CISA certification may be substituted with CIA or CPA credentials "with sufficient, relevant IT audit experience." How much IT audit experience does IA consider sufficient to substitute for CISA? Specifically, will a candidate holding an active CIA with 3+ years of IT-adjacent compliance work (SOC 2, ISO 27001, NIST 800-53) be considered for the IT Senior Auditor role?

A72. From page 4 of the RFP, this position requires four or more years of recent experience conducting IT audits or internal audits, including three years leading IT audits. IA needs to interview resources to ensure sufficient, relevant experience operating as a lead IT auditor.

Q73. The RFP states external staff should have "sufficient tenure with respondent service provider to validate expertise and work product quality." What minimum tenure period does IA consider sufficient, and does this requirement apply equally to subcontracted resources sourced through a vetted professional network?

A73. It is incumbent on the service provider to demonstrate confidence in a given resource's expertise and work product quality, including staff members and subcontracted resources. IA also needs to interview the resource to ensure experience operating as a lead auditor.

Q74. What is IA's typical minimum lead time before activating an audit assignment—i.e., how much notice does IA generally provide to the service provider before external staff are expected to begin fieldwork? This determines whether staff must be held in a dedicated ready-to-deploy capacity.

A74. Once the contract is awarded, the service provider should have a resource ready to work in two to four weeks. In the future, the lead time is 30 to 60 days before the next audit project.

Q75. The RFP estimates fee schedule hours (1,200 IT Senior Auditor, 85 Manager/Director, 80 IT Staff Auditor, 120 Non-IT) as planning estimates and notes "actual hours may vary based on operations and risk." Are these estimates treated as not-to-exceed budget caps per line item, or may actual invoiced hours exceed these figures if IA's audit plan requires it?

A75. The contract will not be amended to add additional hours. Hours are only budgeted for project management purposes. As long as the audit engagement's work still fits within the annual not-to-exceed dollar amount per the contract, email approval from Internal Audit would suffice to change budgeted hours. The annual not-to-exceed amount is a hard stop.

Q76. The RFP requires all costs—including travel and supplies—to be embedded in hourly rates. For staff based outside of Georgia who are required to work in-person in Lawrenceville, does "travel" include airfare, hotel, and per diem for each in-person engagement period, or only local ground transportation once staff are already on-site?

A76. The County will not cover additional expenditures outside of the agreed hourly billing rates paid for work performed. To address the specific examples in this question, travel means time in transit, airfare, hotel, per diem, ground transportation, etc., none of which can be charged to the County.

Q77. The RFP requires pricing to remain firm for the initial contract term and provides blank percentage fields for each of the four annual renewal options. Is there a maximum allowable escalation percentage the County will accept, and will a proposal that locks in flat pricing across all five years be scored more favorably than one proposing modest annual escalations?

A77. There is not a maximum allowable escalation percentage. The renewal rate will be negotiated annually within the percentage indicated. Cost scores are based on year one cost.

Q78. Section D (Understanding & Approach) carries 25 points and asks for examples of "recent, similar engagements" explicitly excluding IT audit work limited to automated scanning. Will the evaluation committee accept federal government IT compliance roles—such as FISMA assessments, Security Authorization & Accreditation work, or continuous monitoring engagements at federal agencies—as directly comparable to the County's CIS-guided IT audit program?

A78. It is incumbent on applicants to illustrate how any engagements are comparable to the nature of IT Audit work described in detail within the RFP. The County's IT audit program requires critical thinking, openness to learning, collaboration, and mental dexterity. It is not a one-size-fits-all or "checklist" audit.

Q79. The RFP does not specify a page limit for the technical proposal. Is there a recommended or expected length for Sections A through E, and do appendices such as resumes, reference forms, and insurance certificates count toward any page guidance?

A79. There is not a limited or expected number of pages in the proposal response.

Q80. Will the County provide scoring feedback or conduct debriefings with unsuccessful proposers after award, and if so, what is the process and timeline for requesting one?

A80. After award, unsuccessful proposers may request a debrief.

Q81. What percentage of work is expected to be onsite vs. remote, and are there minimum onsite requirements per resource?

A81. Remote work is not expected to be the primary service delivery method unless/until a team member's ability to perform and collaborate has been demonstrated on this engagement and IA determines remote work would not hinder collaboration, performance, or quality. IA will discuss the onsite requirements with the winning service provider and requirements may vary based on audit phase and engagement.

Q82. How many IT audit engagements are expected annually, and what is the average number of hours per engagement?

A82. The IT Audit plan includes three to four audits per year. The hours required for each project may vary based on its complexity and IA will collaborate with the winning service provider to estimate hours.

Q83. How are the estimated 1,200–1,400 annual hours typically distributed across engagements and audit phases?

A83. Please see Page 9 of the RFP. For individual engagements, historically 70% of resource hours were allocated to the planning and testing phases.

Q84. Given that automated tools and AI are restricted, what tools or accelerators are permitted for use during audits?

A84. Auditors frequently use Excel, including pivot analysis, and Internal Audit is open to hearing about tools available from submitting service providers if the tools do not have to be run on the County network.

Q85. Can IT Staff Auditors independently perform portions of testing, or must all work be led by Senior Auditors?

A85. **The senior auditor is responsible for external staff's work product quality. IT Staff Auditors may perform portions of testing reviewed by the IT Senior Auditor or, at IA's discretion, reviewed by IA's internal, on-staff IT Audit manager.**

Q86. Is there an estimated annual budget range or target hourly rate range for this contract?

A86. Please see A16.

Q87. Can proposals be submitted via email?

A87. No.

Q88. How does IA prioritize CIS vs. NIST vs. County-specific standards when there are differences or overlaps?

A88. Generally, IA would expect County specific standards to align with CIS. IA would leverage CIS and NIST to develop criteria for evaluating control design.

Q89. Beyond the high-level plan posted online, can IA share which IT domains are most likely to be audited first or most frequently?

A89. No, this depends on annual risk assessments conducted by IA and approvals from the Audit Committee.

Q90. For the estimated 70+ controls annually, does IA expect primarily entity-level, process-level, or technical configuration-level testing?

A90. IA conducts a risk assessment prior to each engagement to determine the appropriate level of testing and/or control design review. Based on this assessment and the current state of controls, controls may be tested at the process level and/or the technical configuration level.

Q91. Can IA provide examples of the "non-IT related auditing services" historically requested under staff augmentation?

A91. Historically, IA's usage of staff augmentation for non-IT related auditing services has been infrequent and minimal. General examples of IA engagements outside the IT audit program are available on the County website here: https://www.gwinnettcounty.com/government/departments/county-administrator/internal-audit/audit-reports

Q92. How frequently does IA typically request short-notice or ad hoc audit support outside the approved audit plan?

A92. It is rare for IA to request that the external service provider work on projects that are not part of the audit plan.

Q93. Can the County confirm the name of the IA project management tool the external staff will be required to use?

A93. The project management portal in place at the time of this RFP is SharePoint. The audit team also uses Teams to collaborate with external staff. Standard templates will be provided for work papers. The portal and platform are Windows-based and on the County network.

Q94. Can the County clarify whether 'in-state presence' requires a permanent Georgia office?

A94. While the service provider does not need to have a permanent physical office space in Georgia, the service provider does need to have existing staff presence in Georgia that is not dependent on the award of this contract.

Q95. Can the County clarify whether annual risk assessment activities are embedded within individual audits or expected as a standalone effort each year?

A95. Risks are assessed at a broad level annually by IA staff and within each audit engagement's planning phase in collaboration with external staff. External staff do not need hours allocated to annual risk assessment efforts.

Q96. Can the County describe its internal Quality Assurance process and the extent of external staff involvement?

A96. IA staff reviews conformance with professional standards each year. This is conducted by a full-time, internal staff member. Audit work is generally conducted in such a way that evidence of conformance results from day-to-day operations. External staff have not been expected to contribute to preparation for internal or external quality assessments.

Q97. Will external staff be expected to support remediation tracking beyond initial validation (e.g., quarterly follow-ups), and should those hours be assumed within the annual estimate?

A97. Currently, IA team members perform remediation tracking activities. IA would normally not expect external staff to support this unless IA is understaffed. Those hours do not need to be included within the annual estimate.

Q98. Is the proposer required to submit the County provided forms exactly as issued, or may the forms be recreated in the proposer's standard formatting provided all required information is included?

A98. The County provided forms should be returned exactly as issued.

Q99. Should the hourly rate for each labor category apply uniformly across all engagements, including non-IT audits?

A99. Yes.

Q100. Are there existing testing templates that the County would like the selected service provider to leverage?

A100. IA will provide templates during onboarding. The external service provider is expected to follow all templates and guidance provided by IA.

Q101. Are there existing reporting templates that County would like the selected service provider to leverage?
A101. Yes, report templates will be shared. For repeat audits, previously issued audit reports will be shared with the external service provider's audit team.

Q102. Will the workpapers be housed in ITS' SharePoint?
A102. The County would like the selected service provider to leverage data and audit work products in secure County storage site or an agreed upon location.

Q103. Will team members be issued County devices to ensure adherence to applicable county policies, or may they utilize equipment provided by the selected **s**ervice provider?
A103. The County will issue a laptop to the designated senior auditor. Other positions will be provided an extranet account to access SharePoint and Teams. Any equipment provided by the selected service provider will need to be secure.

Q104. Can you please confirm the standard payment terms?
A104. Net 30.

Q105. Section II - Scope of Work (Page 3) - Has Internal Audit identified the three to four control areas they will cover in 2026?
A105. The Audit Committee approves a plan each year. For 2026, the flexible plan includes: Internal Firewalls, IT Asset Management, User Access Control, and a post-implementation review of Oracle Fusion.

Q106. Section II - Staffing (Page 3) - Can the County clarify the definition of "automated tools" in this context?
A106. Any analytic, testing, or scanning tools or software that require direct access to the County's network or systems.

Q107. Section II - Staffing (Page 4) – If a team member recommended for the Audit Manager position has CISA, CPA, and 12 years of experience, will that be sufficient instead of the requested CISSP/CISM title?
A107. This would depend on the team member's technical knowledge and expertise. On Page 4 of the RFP, the position documented is IT Audit Manager or IT Security expertise.

Q108. Section II - Deliverables (Page 5) - There is an IA Project Management Tool referenced on Page 5. Please share the name of that tool?
A108. Internal Audit currently uses SharePoint and Teams.

Q109. Professional Services Insurance Requirements - Crime or Fidelity Insurance (Page 15) – A service provider currently maintains a $500,000 crime/fidelity policy and is evaluating the $1,000,000 coverage level. Is the $1,000,000 limit a strict requirement at the time of proposal submission?
A109. It is not required at time of proposal but will be required of the highest scoring service provider prior to award.

Q110. Is this a recompete of an existing contract? If so, who is the current incumbent and what has been the historical annual spend for these services over the last two fiscal years?
A110. 2025 total annual hours were 1,748. The incumbent service provider billed a total of $210,000.
2024 total annual hours were 1,922. The incumbent service provider billed a total of $232,963, which was over budget.

Q111. Will external staff have access to prior audit workpapers and reports to build continuity, or is each engagement expected to start from scratch?
A111. Many engagements may focus on areas that have not been audited in depth before and require largely starting "from scratch." Some audits, however, may leverage prior work papers and reports.

Q112. Of the 1,200–1,400 estimated annual hours, is there a minimum guaranteed number of hours, or is this estimate purely for planning purposes?

A112. There is no minimum guaranteed number of hours. This estimate is for planning purposes.

Q113. If a service provider identifies a high-risk area during a manual review that would be best served by a targeted automated scan (e.g., a specific vulnerability assessment), is there a process to request a one-time exception to the "no automated tools" rule?

A113. IA can assist external staff in communicating with ITS about this. However, the RFP indicates that service providers should assume that running automated scanning tools will not be possible.

Q114. Does the prohibition on Artificial Intelligence apply broadly to all work product (e.g., report formatting/templates), or specifically to the analysis and testing of County data and systems?

A114. The RFP states, "Service providers should assume the use of Artificial Intelligence (AI) will not be permitted in conducting this work." External staff must disclose the nature of any AI assistance they use in the normal course of business or intend to use on County engagements for formatting or narrative drafting purposes. In work papers and reports, all statements must be supported by audit evidence or industry standards (not AI search results).

Q115. Does the County provide read-only access to system configurations (e.g., Active Directory, Firewall rules) to facilitate manual review, or must all data be requested through County staff?

A115. Generally, any read-only access, when available, would be provided to full-time IA staff who work closely with external staff and can facilitate collaborative review with their participation. There may also be observation sessions with ITS.

Q116. Can the County identify the specific "online project management portal" currently used by the Office of Internal Audit (e.g., SharePoint, TeamMate, AuditBoard, etc.)?

A116. SharePoint

Q117. Are external staff expected to facilitate and lead opening/closing meetings with departmental management, or will IA leadership handle those independently?

A117. Typically, opening and closing meetings are conducted by the internal IT Audit manager with external staff in attendance. In rare cases, the IT Senior Auditor may lead the meetings.

Q118. Can the County clarify the typical weekly cadence for on-site presence? For example, are staff expected to be on-site 100% of the time during fieldwork, or is a hybrid model currently the norm for external staff?

A118. Please see A81.

Q119. Can the IT Senior Auditor and IT Audit Manager/Director roles be fulfilled by the same qualified individual, or does the County require these to be separate resources?

A119. If the same individual can fulfill the qualifications and requirements of both roles, IA is open to considering a proposal that proposes the same qualified individual as long as work can be completed within the budget.

Q120. Regarding the "Non-IT Related Auditing Services" (Item #4 in the Fee Schedule), what specific types of operational audits are anticipated (e.g., Procurement, HR, Public Works)?

A120. Please see A91.

Q121. Will the County consider a price adjustment formula (e.g., CPI) for renewal years in lieu of a fixed percentage increase?

A121. No.

Q122. Can the County provide an estimated percentage of work (e.g., 25%, 50%) that has historically been performed remotely vs. on-site for previous engagements?

A122. No, this information may not be a good indicator of future possibilities due to how many factors are involved and any challenges associated with such engagements.

Q123. Does the "no travel reimbursement" clause apply to "other operational locations" that may be significantly outside the two-mile radius of the Gwinnett Justice & Administration Center?

A123. It applies to all locations, but it is rare for travel to extend beyond this radius. The County will not cover additional expenditures outside of the agreed hourly billing rates paid for work performed.

Q124. Will the County accept background checks completed by the service provider within the past 12 months, or are new checks required specifically for this contract?

A124. New background checks are required.

Q125. Can the County clarify whether the scope of this RFP requires service providers to provide only IT audit/advisory services through staff augmentation, or both IT services and IT staffing support?

A125. This RFP is for IT audit/advisory services through staff augmentation. It is not for IT services or IT staffing support.

Q126. Can the County provide additional detail on the expected depth of IT audit engagements (e.g., configuration-level testing vs. policy/process-level review)?

A126. IA expects external staff to go beyond interviewing ITS personnel and reviewing policy documentation. Interviews and policy documentation would only offer insight into the design of a control and its intended operation. As part of IA, external service providers will also need to perform deeper, hands-on testing, which often involves selecting a sample from a population and requesting additional evidence or reviewing configurations.

Q127. While CIS and NIST frameworks are referenced, does the County prioritize any specific framework (e.g., NIST CSF vs. NIST 800-53) for audit alignment and reporting?

A127. The County generally prioritizes CIS. Specific standards may depend on the engagement and criteria needed.

Q128. Does the service provider need to submit resumes of the requested positions or key personnel?

A128. Yes. From page 7 of RFP, the service proivder needs to provide resumes to include background, experience, certification, and qualifications of key personnel that will be assigned to the County.

Q129. How are responsibilities typically distributed between IT Senior Auditors and IT Audit Managers/Directors during engagements?

A129. The IT Senior Auditor conducts the audit, working closely with IA management and consulting the external service provider's Security Expert for additional expertise or guidance as needed.

Q130. Under what conditions would the IT Audit Manager/Director (Security Expert) be required to participate in engagements?

A130. This occurs whenever deeper expertise or additional experience is needed in a technical area. The Security Expert would augment the IT Senior Auditor's knowledge and expertise and participate in walkthroughs and test design. The Security Expert may also need to review work.

Q131. What key performance indicators (KPIs) will be used to evaluate the success of audit engagements?

A131. The primary success factor is work product quality and County satisfaction rather than quantitative attributes, but the County does track budget-to-actual and completion of the audit plan.

Q132. Among the evaluation criteria, what factors will carry the greatest weight in scoring (e.g., methodology, experience, or approach)?

A132. Refer to page 8 of RFP for the scoring points where "Understanding and Approach" has the highest amount of points.

Q133. Should pricing be strictly limited to hourly rates as outlined in the Fee Schedule, or can service providers propose alternative pricing models (e.g., blended rates or role-based pricing structures)?

A133. Pricing should follow the guidelines provided in the RFP.

Q134. Are service providers expected to include all costs (e.g., overhead, tools, administrative support) within the proposed hourly rates, with no additional reimbursable expenses?

A134. Yes.

Q135. How does Gwinnett County's decentralized IT model (central ITS + departmental IT staff) affect audit scoping and coordination for completion of services?

A135. This depends on the audit. IA primarily works with ITS on most audits.

Q136. How would the winning proposal position CIS vs. NIST usage—primary vs. supporting frameworks? Will the winning proposal have the liberty to position accordingly or work with the County in conjunction?

A136. The external service provider would use CIS as primary, but criteria may vary depending on the engagement. The external service provider would work with the County (IA) to determine everything. The external service provider collaborates as part of IA and does not operate with autonomy.

Q137. How will external staff interact with IA's project management tool on a daily basis?

A137. External staff will store non-final/work-in-progress documentation in Teams, communicate with IA staff in Teams on an ongoing basis, and manage the project in a SharePoint team site (the IT Audit site). On the IT Audit site, there is a custom list for the Risk and Control Matrix (RCM) and a data request list. These are interconnected. The IT Audit site provides ITS with visibility into the RCM and allows collaboration.

Q138. What cadence of status updates, issue escalation, and draft review does IA likely expect?

A138. There will be close collaboration with IA on an ongoing, continuous basis, and weekly or biweekly status updates that also include ITS.

Q139. What are the expectations or percentages/time of on-site work for the winning bidder?

A139. This may vary by audit phase and engagement. For example, walkthroughs may be conducted on-site, whereas testing could potentially be performed remotely. The IT Senior Auditor needs to be available for on-site work.

Q140. What does IA likely expect an RCM to look like in terms of depth and format?

A140. IA will provide a detailed template. Fields include but are not limited to risk description, control description (summary), narrative detail, date of walkthrough, control owner, frequency, control category, test procedures, conclusion (descriptive), and control rating.

Q141. How detailed should control narratives be to match prior IA reports?

A141. IA will provide guidelines. Control descriptions should be concise, briefly capturing the control activity or steps performed; the control owner/position performing the activity; frequency; system/tool; and how the control is evidenced. Control narrative detail would include additional detail from the walkthroughs.

Q142. How should findings be tracked, validated, and revisited quarterly?

A142. Currently, IA team members perform remediation tracking activities. IA would normally not expect external staff to support this unless IA is understaffed. Those hours do not need to be included within the annual estimate.

Q143. Where should we acknowledge execution risks (e.g., documentation gaps, scheduling conflicts)?

A143. Execution risks should be discussed or documented with the engagement team during the planning phase of each audit project.

Q144. Has a previous risk assessment been performed? Are there formal enterprise risk management (ERM) processes in place? Would the winning service provider have access to leverage these items upon beginning the engagement?

A144. IA is unable to answer questions about enterprise-level risk management processes. External staff do not need hours allocated to annual risk assessment efforts. IA can share the results of any risk assessments performed by IA. External staff are mostly involved in audit execution, including considering/documenting risks associated with each audit topic on the plan, without a significant role in broader risk-assessment for the enterprise.

Q145. How does the County see responsibilities split between the internal team and the co-sourcing provider for this engagement's scope of work?

A145. Generally, the IT Senior Auditor is expected to conduct the audit work under the close supervision of IA's internal staff with continuous involvement. IA internal staff may share project management responsibilities.

Q146. Can the County share the potential breakdown of the planned co-sourced internal audits/projects by topic (e.g., operational, financial, compliance, IT-related, research-related, construction-related, fraud investigations, etc.)?

A146. The co-sourced internal audits are expected to be IT-related, but other needs could potentially arise. In the past, nearly all of the co-sourced audit work has been IT-related.

Q147. Will previous internal audit documentation (e.g., process documentation, audit results) be available to the successful service provider upon beginning the engagement?

A147. Yes, when available. There may be cases where it is the first in-depth audit of an area which would limit what is available.

Q148. Have there been any significant internal control findings (i.e., management letters/significant deficiencies/material weaknesses) from past internal and/or external audit reviews?

A148. IT Audit results are not shared in public documents since they are exempt from open records on the basis of being IT security related.

Q149. Does the County expect any external audit reliance on internal audit work?

A149. IA does not have insight into future external audit plans. External auditors work with Financial Services and may request our reports, but IA does not know the extent to which the external auditors rely on internal audit work.

Q150. Are information technology processes, policies, and procedures centralized and standardized across systems? If not, please briefly summarize the extent of decentralization/distribution and variation.

A150. Most of the IT audits focus on processes that are largely centralized.

Q151. How many data centers are used to support/host the critical/in-scope systems, and are the data centers maintained and supported internally, or are they hosted and supported by third parties?

A151. IA cannot provide these details about IT operations.

Q152. Please summarize the nature of IT services and applications that are outsourced/provided by service providers (Data center/Cloud Hosting, Help Desk, Security Monitoring, etc.)?

A152. IA cannot provide these details about IT operations.

Q153. Does the County have an existing software solution for internal audit, integrated risk management, data analytics, and/or automation/machine learning that you would like the winning bidder to leverage? If not, is the County interested in the winning bidder providing such solutions?

A153. The current solutions are SharePoint and Teams. Auditors frequently use Excel, including pivot analysis, and Internal Audit is open to hearing about tools available from submitting service providers if the tools do not have to be run on the County network.

Q154. Is there a required timeline or fixed cadence to complete the audits (monthly, quarterly)?

A154. No, timelines for each audit are established during the planning phase.

Q155. What is the average number of audits completed a year? Is the expectation that audits will be completed concurrently?

A155. Approximately three per year, although this may vary depending on scoping and depth. There may be overlap between audits.

Q156. What is the evidence collection policy/guidance to follow (limited sampling or full documentation)?

A156. This may depend on the risk level and nature of the control. Testing often involves sampling. IA will provide further guidance during onboarding.

Q157. Is there a peak period where additional staffing may be required?

A157. There is no set peak period during the year.

Acknowledge receipt of this addendum on Page 10 of the proposal document.

Sincerely,

Dana Garland, CPPB, FOII, NIGP-CPP
Purchasing Manager