INTERNAL AUDIT REPORT FOR

IT Governance

Gwinnett County Government
Audit Plan Year 2022

November 22, 2022

Gwinnett

GWINNETT COUNTY
INTERNAL AUDIT DIVISION
75 Langley Drive | Lawrenceville, GA 30046
O: 770.822.7757 | F: 770.822.7725
GwinnettCounty.com

Auditors: Jenna Kim, CFE, Internal Auditor
Leslie Villanueva, CISA, CRISC, IT Audit Division Director

Distribution:

To: Dustin Williams, Office of Strategic Excellence Director

CC: Tracy Arner, CPA, Gwinnett County Audit Committee
Kirkland Carden, Board of Commissioners – District 1, Gwinnett County Audit Committee
Tiana Garner, Clerk of Court, Gwinnett County Audit Committee
Ben Ku, Board of Commissioners – District 2, Gwinnett County Audit Committee Chairman
Teresa Reese, CPA, Gwinnett County Audit Committee
Glenn Stephens, County Administrator, Gwinnett County Audit Committee
Maria Woods, CPA, Deputy County Administrator/CFO, Gwinnett County Audit Committee

Theresa Cox, Deputy County Attorney
Dorothy Parks, CIO/Department of Information Technology Services Director

This report is intended solely for the individuals contained in the distribution list. Do not send to any other recipients without written authorization.

Table of Contents

Background & Scope

The Department of Information Technology Services (ITS) maintains a complex network infrastructure to provide quality technology services for several agencies and 14 administrative departments within Gwinnett County Government (the County). ITS has six divisions with 145 authorized positions that provide these services, supplemented by outside professional services and contracts. Their goal is to provide reliable automated business solutions with tangible benefits to agencies, departments, and residents. To be successful, it is critical that decisions regarding technology investments and use of resources are collaborative and align with Board of Commissioners (BOC) priorities. The Department of Financial Services Office of Strategic Excellence (OSE) maintains policies and procedures to support countywide resource alignment, performance management, and continuous improvement. The OSE Systems Solutions team focuses on these goals as they pertain to IT resources. The County initiated IT purchase orders (POs) totaling approximately $35 million during the audit period January 1, 2021, to May 15, 2022.

In January 2020, the County Administrator adopted Policy CA-214 (the Policy) to promote the effective and efficient use of technology in carrying out the County's strategic priorities. The Policy established an IT Governance Model to evaluate, select, and prioritize projects. Departments and ITS Business Relationship Managers (BRMs) must justify proposed projects based on expected benefits, implementation risks, and costs in a business case format. They submit business cases to OSE. OSE Systems Solutions reviews them for completeness, among other criteria, before forwarding those with total costs of more than $5,000 and/or 40 ITS implementation hours to the IT Functional Governance Team (the Functional Team) for review and concurrence. The Functional Team is comprised of ITS deputy directors and departmental liaisons. They assess the technical feasibility and business value of business cases. If proposals exceed $100,000 and/or 40 ITS implementation hours, they undergo another review by the IT Oversight Group (the Oversight Group), comprised of County executive leaders. The Oversight Group evaluates business cases based on their expected benefits, strategic alignment, and available resources. All administrative departments must comply with the governance framework. Agencies may voluntarily comply with the requirements. OSE is responsible for managing governance program processes.

The purpose of this audit was to assess on a sample basis departmental compliance with the Policy and the adequacy and effectiveness of control activities that are designed to provide reasonable assurance of achieving governance objectives. Internal Audit (IA) interviewed employees and reviewed documentation on a sample basis for the audit period. We reviewed procurement card transactions in a separate audit and excluded them from our samples. We believe the evidence provided a reasonable basis for our assessment. See **Exhibit A** for a summary of our audit procedures.

Assessment

Departmental compliance with the Policy was reasonable given the maturity of the program but could improve. Most instances of non-compliance were related to Policy misinterpretation. IT governance activities generally provided reasonable assurance of achieving oversight objectives. We identified four opportunities for improvement.

Recommendations

1. Limited number of appointees in the Oversight Group.

The Oversight Group's objectives are to ensure IT projects align with BOC's priorities and provide tangible benefits. They also prioritize projects based on their importance to the County and efficient use of resources. Member decisions must be based on a comprehensive understanding of County operations to be effective. The IT Governance Model recommends the Oversight Group includes high-level appointees from agencies, County Administration, Financial Services, OSE, and ITS, but does not outline official requirements. As of the end of fieldwork, there were three members: the CIO, Deputy County Administrator/CFO, and Chief Court Administrator.

RECOMMENDATION

The Oversight Group should appoint members from Financial Services and OSE. Although not included in the model, we also suggest one or two appointments from other departments. OSE should propose Policy updates to include minimum membership requirements. The Policy should also address how and by whom members are appointed.

Management Response (OSE)

Management agrees with this recommendation and will include clarifying membership language in upcoming suggested revisions to the policy.

2. Some business cases lacked sufficient information, and submission processes could be improved.

Departments and BRMs must justify their project or purchase requests. OSE adopted a standard business case form for submitting proposals for evaluation. The form ensures departments submit coherent requests with core information about expected project outcomes for the committees to evaluate. The core information includes a summary of the opportunity or problem, justification, BOC priorities, solution options with risks and benefits, and expected return on investment (ROI). IA identified a population of 71 business cases and reviewed content for compliance with submission criteria. Departments completed business cases in the standard format with relevant information but sometimes lacked required content. We also evaluated the adequacy and effectiveness of business case processes. Overall, we found no major unexplained instances of non-compliance, but we observed some opportunities for improvement.

RECOMMENDATION

See **Exhibit B** for a summary of improvement opportunities and recommendations.

Management Response (OSE)

Management agrees with the opportunities identified and will address those opportunities through proposed policy revisions and/or process changes in partnership with ITS.

Management Response (ITS)
Overall, ITS Management agrees with IA's improvement opportunities. Additionally, ITS Management believes the completion of business cases would be most beneficial to the County if efforts were more focused on core strategic objectives and associated IT investments. The current policy requirements as to when a business case is required are quite restrictive and have led to operational inefficiencies and delays in IT business operations as business cases are required for small purchases and minimal staff resource allocations. The current thresholds of 40 hours of work and/or $5,000 in expenditures in a technology arena are extremely low thresholds for requiring such overhead as it pertains to business case development and oversight in managing day-to-day IT-related business operations. These thresholds should be raised substantially so that both ITS and OSE resources are focusing on the highest value and most impactful IT investments for the County. ITS has previously proposed such recommended thresholds to OSE that would allow for a more efficient process that would minimize unnecessary overhead to operate.

IA Comment
IA encourages ITS to comply with Policy requirements as currently defined, including improvement opportunities, while working with OSE and senior management to resolve ITS concerns about business case thresholds.

3. Compliance activities may not promote adherence to the IT Governance Model.

The Policy requires departments to channel most proposed IT purchases, among other requests, through the IT Governance Model. OSE relies on departments to properly identify and submit requests for governance review. To evaluate departmental compliance, IA selected a judgmental sample of 31 eligible purchase orders (POs) and sought evidence of governance review for the related contracts or projects. There were 14 (45%) POs without evidence of governance approvals. We also vouched an additional 14 eligible contracts to governance documentation and found two (14%) without governance approvals. At the time of the audit, there were no formal control activities for certifying governance committee approvals prior to procurement.

Financial Services Purchasing Division (Purchasing) reviews contracts prior to consummation to validate compliance, but they are not always aware of purchases that are associated with active or legacy contracts or renewals. IT POs originating in any department automatically route to ITS, but not all of them workflow to Purchasing or OSE. OSE and Purchasing should define compliance activities and use workflows or automated notifications when feasible to ensure completeness of compliance reviews. Also, we found departments were unfamiliar with or misinterpreted IT Governance Model requirements. For example, some employees did not know contract renewals with additional software licenses or enhanced functionality required governance committee approvals, contributing to non-compliance.

RECOMMENDATION
OSE and Purchasing should formalize the step of verifying governance approvals prior to proceeding with IT procurement. To improve departmental compliance, consider providing an electronic intake form to collect pertinent information about prospective IT purchases and compute governance requirements. OSE should also conduct departmental training sessions to improve awareness and periodically review transactions on a sample basis for compliance. OSE should use results to improve educational and compliance activities.

Management Response (OSE)
Generally, the governance process as designed should occur before any procurement activity takes place with purchasing verifying governance approval before acting on IT-related procurements as a compliance check. While many business cases lead to new procurements, the governance process is not intended to be an approval step in the procurement process. In some cases, the options pursued will be accomplished utilizing existing resources without the need for a new procurement. That said, management agrees that improved coordination between ITS, OSE, Purchasing, and departments is needed to improve awareness and compliance with the policy.

IA Comment
IA understands and agrees governance should occur before procurement. We recommend formalizing Purchasing's compliance check to verify governance approvals occurred prior to acting on IT-related procurements.

Management Response (ITS)
ITS Management agrees with IA's recommendations. It is imperative that ITS be involved early and often in the vetting and procurement of technology solutions. This is critical to the success of IT operations and the County as unvetted procurements can have an immediate impact on IT resources to implement and maintain such solutions. Additionally, considering the cybersecurity threat landscape, all technology solutions require vetting by the Cybersecurity Department within the ITS organization. Lastly, small purchases such as the procurement of additional licenses associated with an implemented and supported solution should pass through IT Governance but should do so in a timely manner with only the necessary data to make County best interest decisions. Business cases for such items are an inefficient use of County resources and pull limited staff away from more critical/high-risk efforts.

4. IT governance activities may not include all areas that impact BOC priorities and services.

Key objectives of the County's IT Governance Model include ensuring expenditures align with BOC priorities and provide measurable benefits. IT governance committees follow a structured decision-making process for approving and prioritizing business requests for projects, software, hardware, and services to achieve these objectives. The scope, however, does not include other important IT decisions that impact BOC priorities and departmental services. These include strategic planning, risk management, staffing, and service delivery. At a minimum, IT governance committees should know the status and results of these activities. The additional oversight will require clarifying responsibilities for accumulating and summarizing relevant information for committee use. Governance committees will need to establish accountability measures and communication strategies for each area.

RECOMMENDATION
Senior management should consider expanding the IT Governance Model to include strategic planning, risk management, staffing, and/or service delivery. ITS and OSE should better define their responsibilities for supplying the required information, including data frequency, format, and level of detail. The communication plan should include procedures for soliciting feedback from all stakeholders on governance processes.

Management Response (OSE)
Management agrees with the recommendation and will work with ITS to gain more insight into roadmaps, resource availability, project management status, etc. This will further strengthen the committee members' decision making and prioritization of projects.

Management Response (ITS)
ITS Management partially agrees with IA's recommendations. ITS Management sees value in an IT governance committee reviewing and managing enterprise risks as well as providing insight and direction on the strategic selection, prioritization, and implementation of IT investments. However, adding IT governance oversight to areas of ITS operations such as staffing, and service delivery would only hinder IT operations and the ability for ITS to become more agile and nimble in an ever-evolving industry. Challenges already exist to recruit talented IT professionals and service delivery metrics can be reported out of the CIO office to provide visibility into service delivery effectiveness. Additionally, such oversight around areas like staffing and service delivery minimizes the purpose and authority of having IT leaders such as the ITS CIO and Deputies whose experience and concentration are geared to drive IT operational efficiencies.

IA Comment
IA does not advocate adding processes that hinder operations. We encourage ITS and OSE to work collaboratively to ensure governance oversight of pertinent areas.

Other Consideration

IA observed an opportunity to improve certain business activities based on best practices and included an advisory comment for management consideration only. Management responses or corrective action plans are optional. The advisory comment is as follows:

> OSE manages governance records via the Management Framework (MFA), an online portal that has departmental project dashboards and serves as the document retention site for business cases. BRMs and departments upload business cases to the site, usually in unprotected Word documents. The current review workflow is manual and lacks sufficient safeguards to secure content, manage changes, and certify that governance committee approvals were based on the latest version. Employees may edit, delete, or replace business cases or entire MFA project records without detection because there are also no role-based restrictions. We suggest OSE consider using DocuSign to secure documents and automate workflows, including committee approvals. At a minimum, OSE should secure documents with evidence of committee approvals before uploading them to the MFA, restrict MFA user capabilities based on job responsibilities, and develop version control protocols for documents.

Exhibit A: Summary of Audit Procedures

IA performed the following procedures to evaluate the adequacy and effectiveness of compliance and control activities:

- Interviewed Functional Team members, Oversight Group members, ITS Business Relationship Managers (BRMs), and ITS managers who internally review business cases before submission. Inquired about governance requirements, the purpose of review activities, risks, and pain points.
- Interviewed Purchasing and Budget personnel to understand their involvement in key control activities related to IT-related purchases and budgeting.
- Reviewed the Policy, Governance Model Document, member lists for both IT governance committees, and other documents for scope and consistency (**Recommendation 1**).
- Conducted best practice research and reviewed IT governance publications from ISACA and the Institute of Internal Auditors.
- Reviewed a population of 71 business cases submitted to OSE during the audit period and identified 22 that included fewer than three options. Inquired of BRMs and OSE to understand why the business cases did not include a third option. Out of the population of 71 business cases, selected a random sample of 17 cases to assess Policy compliance and confirm outcomes were consistent with governance committee voting records. Reviewed business case content, including metrics and risks (**Recommendation 2**).
- Examined a stratified random sample of 167 IT-related POs from the audit period and determined that 31 (approximately $8 million) required IT governance oversight. Reviewed supporting documentation for 31 POs to verify IT governance approval according to the Policy, with 14 exceptions. Reviewed 14 IT-related contracts made during the audit period that should have gone through IT governance, with two exceptions (**Recommendation 3**).
- Interviewed OSE Systems Solutions and ITS senior management to determine IT governance objectives, requirements, procedures, risks, and key controls. Walked through key activities to confirm understanding and validate procedures (**Recommendation 4**).
- Identified 13 withdrawn business cases and inquired with BRMs to understand the business rationale for withdrawals.
- Read the Oversight Group's quarterly meeting minutes and observed a quarterly Oversight Group meeting.
- Obtained 2022 Capital Budget Requests and Capital Budget Review Committee recommendations. Reviewed funding status of IT governance projects. Reviewed the Capital Budget Review Committee's list of recommended projects for IT governance statuses, without exception.

Exhibit B: Business Case Recommendations

Business Case Content	Improvement Opportunities
Options Departments and BRMs must identify a minimum of three options to meet their business needs or remediate issues, including the current state for comparison purposes. The options should include expected benefits, costs, and implementation risks. Departments should also identify and justify the recommended option.	Twenty-two business cases out of 71 contained only one option in addition to "Do Nothing." According to management, there were no viable options to consider for these projects, but most business cases did not explain. Business cases should describe circumstances that preclude multiple options. OSE should return cases for revisions, when necessary, before sending them to committees.
Benefit Measurement Business cases should include a review plan for determining whether the County realized expected benefits. The plan should identify who is responsible for reviewing project results, and how they will measure benefits and evaluate performance. Cases justified by expected business benefits rather than direct financial returns such as ROI should include appropriate key performance indicators (KPIs).	Business cases often lacked key performance indicators (KPIs). Also, there were minimal efforts to validate expected costs against actuals. Business cases should include a benefits review plan that addresses accountability, measures, ownership, and outcomes, including user satisfaction. Departments and OSE should periodically report results to the Oversight Group.
Risks The business case requires departments and BRMs to identify and analyze all potential risks with solutions. Although not required, the risk analysis should include assumptions, likelihood of occurrence, impact, and viable mitigation plans. Management must provide quarterly updates to the Oversight Group about project risks.	IA selected a judgmental sample of 17 business cases to assess completeness. Eight cases omitted risks related to data migration, software capacity, major process changes, or other matters. Management omitted risks from their quarterly updates to the Oversight Group. Departments and BRMs should meet with relevant business owners to identify important operational risks and mitigation plans. Cases should include this information with a list of impacted departments. The Management Framework should track risk changes throughout the life of the project. Oversight Group updates should include risk statuses.

Business Case Process	Improvement Opportunities
Managing Submission Requirements OSE maintains standard forms and processes to facilitate the submission and disposition of business cases. The Policy allows OSE to modify submission requirements based on request type and scope to facilitate efficient dispositions.	OSE rarely modified business case content requirements to promote efficiency or completeness. Examples include requests relating to existing hardware or software. OSE should modify requirements for certain scenarios or provide written guidance on acceptable modifications to the standard requirements to promote efficiency. The guidance should include examples.
Review for Redundancies The Policy requires OSE to identify potential redundancies in hardware and software in the County's existing environment as part of their initial review of business cases. This is to ensure departments include existing or similar County assets as options in the business case.	OSE did not document redundancy reviews. Also, they did not check hardware-related business cases for potential redundancies. OSE should complete a checklist to document their review procedures. OSE should obtain comprehensive hardware and software inventories from ITS to improve detection.