INTERNAL AUDIT REPORT FOR

Continuity of Operations
Gwinnett County Government
Audit Plan Year 2023

July 11, 2023

Gwinnett

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

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

Distribution:

To: Please see the following page

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

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

Distribution:

To: Greg Swanson, Office of Emergency Management Director

Buffy Alexzulian, Financial Services Director
Cleophas Atwater, Sheriff's Office Chief
Christopher Ballar, Probate Court Judge
Philip Boudewyns, Chief Court Administrator
Fred Cephas, Fire Chief
Lewis Cooksey, Transportation Director
Matthew Dickison, Planning and Development Director
Tina Fleming, Community Services Director
Tiana Garner, Clerk of Court
Kimberly Jenkins, Magistrate Court Executive Director
Darrell Johnson, Warden
Mike Ludwiczak, County Attorney
Adrienne McAllister, Human Resources Director
J.D. McClure, Police Chief
Denise Mitchell, Tax Commissioner
Angelia Parham, Support Services Director
Dorothy Parks, Information Technology Services Director
Rebecca Shelton, Water Resources Director
Joe Sorenson, Communications Director
Michelle Vereen, Child Advocacy and Juvenile Services Director

Table of Contents

Background & Scope

Gwinnett County (the County) provides essential public services that must continue in the event of natural or man-made disasters that damage critical infrastructure or impair normal business operations. Though catastrophic events may be infrequent, agencies and departments must plan for maintaining critical governmental services under any circumstance. Each agency and department maintains their own continuity of operations plans (COOPs). They have a designated COOP Planner for coordination and project management. The County subscribes to a continuity planning system, Boldplanning.com, to assist in the creation and maintenance of COOPs. It provides standard templates and serves as a central repository. The Police Department's Office of Emergency Management (OEM), among many tasks associated with emergencies, assists agencies and departments with continuity planning. They also provide recovery assistance after an incident and non-mandatory training through a third party.

Continuity planning is an important business practice. It should be continuous with a focus on maintaining decision-making and operations under various operational scenarios such as the inability for personnel to access the Gwinnett Justice and Administration Center, other important government infrastructure, information technology (IT) services, critical data, or sufficient human resources. Plans should incorporate interagency and interdepartmental dependencies for sustaining operations. Management must periodically confirm plan validity through desktop exercises, tests, and inspections. The Federal Emergency Management Agency (FEMA) maintains generally accepted guidelines for continuity planning by federal agencies which OEM and many local governments reference. These guidelines stipulate plans should be tailored for individual needs, but they must incorporate certain key elements to be valid. The key elements applicable to the County are alternate facilities, delegations of authorities, essential functions, human resources, interoperable communications, succession planning, test, training, and exercise program, and vital records and databases. See **Exhibit A** for descriptions of FEMA key elements.

The purpose of this audit was to evaluate the adequacy of the County's planning program for maintaining operations in the event of business disruptions. Internal Audit (IA) inspected documented COOPs for relevance and compared content to FEMA's framework for completeness.   IA also interviewed management and observed certain planning activities for the audit period January 2022 through February 2023 to confirm our understanding of them. We believe the evidence provided a reasonable basis for our assessment. The District Attorney's Office was excluded from this review. The Department of Child Advocacy and Juvenile Services is the County's newest department and did not yet have a COOP at the time of the audit.

Assessment

The County demonstrated the capability to successfully coordinate emergency responses and maintain critical services during the COVID pandemic, but management must plan for a wide range of potential disruptions to operations which may be dissimilar to a pandemic. COVID disrupted operations primarily because of human quarantines and resource shortages rather than physical damage, widespread IT network downtime (ransomware), or power outages for example which may require different responses. Agencies and departments purportedly maintained continuity of operation plans

for hazards other than COVID. Many were informal or otherwise unavailable for inspection. Departments must plan for their specific operations, but the County's preparedness for local or widespread disruptions would benefit from improved coordination, departmental collaboration, and a generally agreed upon baseline framework to promote completeness. This should include agreement on the best tools to easily facilitate planning and documentation. Also, IT network performance will impact almost all continuity plans since individual application recovery periods will primarily determine which manual procedures will be needed to continue operations and for how long. All departmental plans for continuing operations should incorporate relevant aspects of IT's service level commitments for disaster recovery. We made three recommendations to improve the viability and effectiveness of COOP planning.

Recommendations

1. **Many COOPs kept in the web portal were incomplete or obsolete.**

   The County engaged BoldPlanning, Inc. in 2008 to facilitate preparation of initial COOPs. The vendor provided planning software, templates based on FEMA standards, and voluntary training programs. The County still uses their services. Several agencies, departments, and divisions continue to document COOPs in Boldplanning.com. There were 38 in the portal as of the end of fieldwork. See **Exhibit B** for details. OEM currently coordinates planning activities and annual vendor training, but each agency and department is responsible for content. IA reviewed all documents to ensure they were current and contained key planning elements per FEMA guidelines. Though agencies and departments purportedly maintained protocols to continue operations in the event of an emergency, plans kept in the system were generally obsolete and excluded key FEMA elements. Planners did not provide any alternative COOP documents for review. The following is a summary of some of the more important improvement opportunities based on the available documents. See **Exhibit C** for a summary of results by key elements.

   - Thirty-five (92%) did not contain evidence of COOP-related exercises or tests to validate recovery strategies. Management must test their plans to ensure they are complete and accomplish operational and service goals.

   - Thirty (79%) did not address delegations of authority and twenty-three (61%) lacked complete succession plans. While management may know order of succession and delegations, they should be written and accessible by all personnel to minimize potential misunderstandings during an emergency.

   - Fifteen (39%) did not contain valid alternate work facilities or lacked sufficient details regarding telecommuting capabilities. Alternative worksites and equipment requirements may change. They should be documented and periodically evaluated for relevance.

   The results are based on available documents, and they may not necessarily reflect preparedness given the tendency of some departments to rely on unformulated plans.

RECOMMENDATION

We cannot overstate the importance of maintaining written COOPs in a central repository. Employees can easily access plan content to better understand expectations and procedures for maintaining critical operations during business interruptions. They provide agencies and departments with the means to better coordinate responses with other departments. Planners can more effectively test continuity strategies to remediate deficiencies and prevent them from becoming stale.

OEM should work with agencies and departments to establish baseline content requirements for COOPs that will promote successful outcomes. OEM should also coordinate and monitor the County's COOP program to ensure plans meet baseline requirements and remain current. We encourage department leaders and OEM to periodically meet to share best practices, review operational changes or dependencies if any, and discuss potential impediments. Planners should periodically re-evaluate plan content to ensure completeness, readability, and relevance. Planners should also conduct regular exercises to validate plan accessibility and recovery strategies. Employee training will promote effective plan execution.

Management Response (OEM)

OEM is committed to working closely with agencies and departments to establish a collaborative approach that promotes successful outcomes and facilitates effective coordination. To address the recommendation, OEM will establish a continuity planning team consisting of representatives from county departments. This team will work together to accomplish the following objectives:

A. Create an overall continuity strategy: The continuity planning team will develop a comprehensive strategy that encompasses the specific needs and requirements of our organization.

B. Identify applicable continuity regulations or requirements: We will diligently identify existing continuity regulations or requirements that are relevant to our organization. In cases where specific requirements are absent, we will identify continuity guidance and principles that align with the continuity strategy.

C. Define continuity program planning roles and responsibilities: We understand the importance of clearly defining roles and responsibilities within the continuity planning process. The team will collaborate to identify and assign these roles, ensuring that all relevant stakeholders are actively engaged.

D. Evaluate continuity planning tools and provide recommendations: We will thoroughly assess the effectiveness of our existing continuity planning tools and make appropriate recommendations for updates or revisions. This evaluation will help us ensure that our tools align with industry best practices and support the organization's needs.

E. Establish a schedule for plan evaluation and revision: Recognizing the dynamic nature of our operational environment, we will establish a schedule for the regular evaluation and revision of continuity plans. This iterative process will enable us to keep plans current, relevant, and responsive to potential challenges.

F. Implement a corrective action program: To continuously improve our continuity capabilities, we will create a corrective action program. This program will help us identify areas for improvement through reviews, exercises, and real-world incidents, allowing us to implement necessary measures effectively.

We understand the importance of working collaboratively with department leaders and relevant stakeholders, fostering a culture of shared knowledge and best practices. Periodic meetings will be organized to facilitate the exchange of information, review operational changes or dependencies, and address potential impediments. Furthermore, we recognize the critical role of employee training in promoting effective plan execution. We will support department-led training programs to ensure that employees are equipped with the necessary knowledge and skills to support the successful implementation of COOPs.

2. Recovery strategies do not incorporate IT operational dependencies.

Agencies and departments rely on IT network operations to provide services to the public. Although the Department of Information Technology Services (ITS) maintains safeguards, the County's network may be vulnerable to cybersecurity attacks such as ransomware, other denial of service attacks, and physical damage which could disrupt network availability. Agencies and departments must identify alternatives to County network solutions such as manual procedures or vendor hosted services for a period. Any network alternative is dependent on ITS's disaster recovery plan (IT-DRP). Expected network recovery times will inform resource requirements for alternative procedures. For example, the ability to telecommute at scale depends on the number of available laptops, VPN capabilities, and IT support services. Planners must incorporate key dependencies from the IT DRP into their recovery strategies to avoid transition problems. Agencies and departments should be involved in testing backups when applicable.

Currently, most COOPs do not incorporate IT DRP dependencies or contemplate limited network availability. Some COOPs listed vital records but not how they would be accessed and used in the event of a system disruption or how functions would continue without the records. In addition, ITS does not have a formal IT DRP with a comprehensive strategy for resuming critical IT systems that planners can use. While ITS may have backup strategies and other plans related to disaster recovery, a comprehensive IT DRP is necessary for coordination of resources and recovery activities.

RECOMMENDATION

Generally, agencies and departments should periodically evaluate all critical infrastructure needed to sustain public services and ensure there are alternatives in case of limited access or functional impairments due to emergencies. OEM should include these considerations in guidance and instructions related to COOP planning. Planners should re-evaluate all infrastructure dependencies at regular intervals to ensure COOPs remain current and comprehensive. Regarding IT operational dependencies, ITS should complete and maintain a disaster recovery plan (DRP) and distribute it to planners so that they can incorporate relevant components into their COOPs. Planners should consider service-level agreements with ITS to clarify any critical dependencies excluded from the IT-DRP that may impact the scale and duration of alternative procedures in the event of emergencies. OEM, ITS, and department leaders should periodically meet to review data recovery performance goals and their potential impact on maintaining operations (see **Recommendation 1**).

Management Response (OEM)
OEM agrees with the recommendation regarding the periodic evaluation of critical infrastructure to sustain public services and the need for alternatives in emergencies. We acknowledge the importance of incorporating these considerations into our guidance and instructions related to COOP planning. OEM will work closely with agencies and departments to ensure that their COOPs include comprehensive evaluations of infrastructure dependencies. By integrating these evaluations at regular intervals, we can ensure that COOP plans remain current, robust, and capable of addressing potential functional impairments or limited access. It is important to note that the actions recommended will be incorporated into the overall continuity strategy outlined in our response to the first recommendation. By establishing a continuity planning team that includes representatives from county departments, we can ensure effective collaboration and coordination, resulting in a comprehensive approach to COOP planning.

Management Response (ITS)
DoITS agrees with this assessment and is aware of the improvements needed. For the 2023 budget cycle, DoITS requested and was granted funding for a contractor to create a formal, documented disaster recovery plan. This plan will require input from County departments to understand their needs and priorities. Completing this deliverable will clarify for senior leadership the timing expectations around recovering systems in the event of a disaster as well as how much data loss should be expected if reverting to a previous backup is necessary. These timelines can then be used to make decisions about continuity planning within the departments.

3. **Coordination between agencies and departments is unformulated.**

   Though agencies and departments have their own COOPs, there were no formulated plans for maintaining essential functions and other constitutional activities during significant disruptions. Agencies and departments often depend on each other and third parties to provide critical services and must coordinate their recovery activities to successfully migrate to alternative processes and locations. The following are some examples where the County could improve continuity of operations oversight and coordination:

   - The BOC and other constitutional officers must continue important governance activities such as contracting for services on behalf of the County, overseeing budget matters, resolving zoning appeals, conducting court proceedings, and providing physical security. There should be a government recovery plan to ensure critical governance activities continue during extended business disruptions or damage to critical infrastructure.

   - Many agencies and departments rely on each other or vendors for critical services. Sheriff provides security for Court operations. Vendors provide inmate healthcare and food services for prisons. There are many more interdependencies that departments should integrate into COOPs to prevent service shortfalls in the event of an emergency.

   - According to COOPs, several departments identified the same building as an alternative work site. This could have posed capacity challenges for that building, but certain departments intended to use telecommuting instead and had not updated their COOPs to reflect these changes.   OEM should review all COOPs and assess whether there is a chance occupancy could exceed capacity under certain circumstances and whether departments must use other alternative work arrangements. There may be other joint capacity or resource availability restrictions that may similarly apply.

- The County lacks policies or uniform standards for operational continuity plans. Also, agencies and departments appear to voluntarily maintain valid COOPs in the central repository if at all. The OEM serves in an advisory role for continuity planning and recovery activities, but there is no single body composed of members from agencies and departments to oversee continuity planning from a county-wide perspective.

RECOMMENDATION

OEM should work with County Administration to evaluate the feasibility of establishing an emergency and continuity of operations committee with OEM as an ex officio member. Committee members should include agency and department leaders to oversee COOP coordination, quality, and compliance with general standards. The committee should also propose general standards for continuity planning for the County Administrator's consideration. We also suggest the committee, among other responsibilities, sponsors joint desktop exercises or other activities to validate county-wide continuity strategies.

Management Response (OEM)

OEM agrees with the recommendation regarding the formation of a collaborative team and will incorporate this into the overall continuity strategy outlined in our response to the first recommendation. By establishing a continuity planning team that includes representatives from county departments, we can ensure effective collaboration and coordination, resulting in a comprehensive approach to COOP planning.

Other Considerations

IA observed opportunities to improve certain business activities based on best practices and included advisory comments for management consideration only. Management is not required to provide written responses or corrective action plans. The advisory comments are as follows:

- Bold Planning, Inc. provides an annual refresher workshop for planners as a part of their contractual responsibilities. IA asked 25 planners whether the annual workshop met their expectations. Twelve (48%) stated the workshop did not meet expectations. They wanted to conduct tabletop exercises with other agencies and departments to validate coordination and identify interdepartmental issues. They also wanted to review their COOPs in training sessions to validate plan content. OEM needs to assess the quality of workshop content and make any necessary changes to improve usefulness. Also, some planners were not aware of workshops. OEM should send workshop dates to all agencies and departments to improve participation.

- Many planners thought online COOP templates were too cumbersome to use. For instance, they cannot directly modify plan content. They enter changes into central data fields which must then be imported into the plan. OEM should spearhead software functionality reviews by users and the vendor to enhance usability.
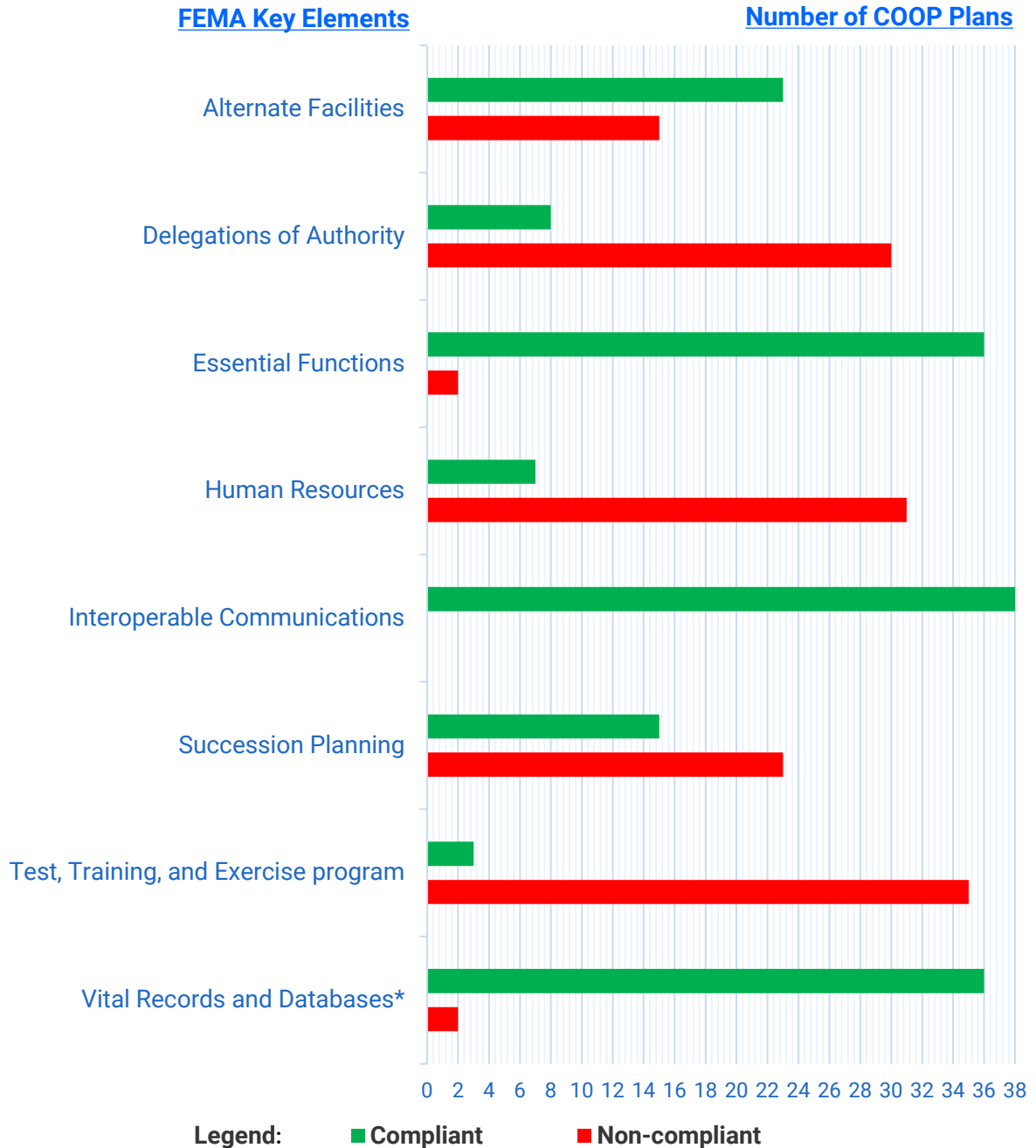
Exhibit A: FEMA Key Element Descriptions

FEMA Elements	Purpose
Alternate Facilities	To identify a location and carry out essential functions when the primary facility is unavailable.
Delegations of Authority	To identify individuals who are currently responsible for the execution of contractual agreements, leave authorization, purchasing requisitions, and travel authorization, at a minimum and individuals who are authorized to act on behalf of acting agents for the specified functions above.
Essential Functions	To identify functions that must be continued in all circumstances to provide vital services.
Human Resources	To continue to perform the essential functions with reduced staffing in emergencies. Agencies and departments should identify employees who are capable to support continuity operations during emergency situations, and their roles and responsibilities during emergencies.
Interoperable Communications	To ensure the capability to communicate internally and externally.
Succession Planning	To provide for the orderly and predefined assumption of leadership during an emergency. Agencies and departments should document the succession plan to ensure they immediately adapt and manage the impact of the event that any officials are unavailable to execute their duties.
Test, Training, and Exercise Program	To ensure that the COOP plan is adequate and viable to support the continued execution of essential functions throughout the duration of a COOP situation.
Vital Records and Databases	To identify electronic and hard copy documents, files, and other materials that are vital to the departments and agencies and their operations.

Exhibit B: Agency and Department COOPs

Department and Agency	Number of COOP Plans
Clerk of Court	1
Communications	1
Community Services	6
Corrections	1
County Administrator's Office	1
Court	1
Financial Services	1
Fire & Emergency Services	1
Human Resources	1
Information Technology Services	1
Law	1
Magistrate	1
Planning & Development	1
Police	8
Probate Court	1
Sheriff	5
Support Services	3
Tax Commissioner's Office	1
Transportation	1
Water Resources	1
Total	**38**

Exhibit C: COOP Review Results

FEMA Key Elements   **Number of COOP Plans**

Legend: ■ **Compliant**   ■ **Non-compliant**

* See Recommendation 2.