Brookhaven
GEORGIA

CITY OF BROOKHAVEN

RISK MANAGEMENT REPORT – INFORMATION TECHNOLOGY GENERAL CONTROLS

AUGUST 31, 2021

NICHOLS CAULEY
Assurance | Advisory | Tax

Table of Contents

NICHOLS, CAULEY & ASSOCIATES, LLC

3550 Engineering Drive, Suite 250
Peachtree Corners, Georgia 30092
404-214-1301 FAX 404-214-1302
atlanta@nicholscauley.com

City Management
City of Brookhaven
Brookhaven, Georgia

We have performed certain operational and compliance procedures, which were agreed to by the City of Brookhaven (City) and the City's management (specified parties), in compliance with the American Institute of Certified Public Accountant's Consulting Standards and Rule 101 of the Code of Professional Conduct. These procedures were performed solely to assist you in evaluating the City's Information Technology (IT) general controls, specifically: Management, Business Continuity/Disaster Recovery, Information Security, and Outsourcing Technology Services. The IT general controls relate to overall data processing activities and information technology activities.

The City's management is responsible for maintaining an adequate control environment and risk management program, and for maintaining compliance with established policies, procedures, and any regulatory requirements. Our responsibility was to evaluate and assess the adequacy of information technology related internal controls and related risk management activities. The sufficiency of these procedures is solely the responsibility of those parties specified in the report. Consequently, we make no representation regarding the sufficiency of the procedures performed for the purpose for which this report has been requested or for any other purpose.

We were not engaged to, and did not, perform an audit, the objective of which would be the expression of an opinion on the City's financial statements or specified elements, accounts, or items thereof. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the use of the specified parties listed above and applicable regulatory authorities and is not intended to and should not be used by anyone other than those specified parties.

Nichols, Cauley + Associates, LLC

Atlanta, Georgia
August 31, 2021

Executive Summary

The procedures performed along with this report have been completed in conjunction with management. This report is intended solely for the use of City management and should not be used by anyone other than the specified parties.

Procedure Summary

The following is a summary of the controls evaluated during our review along with any reportable exceptions identified.

Area	Controls Reviewed	Functioning	Exception(s)
Management	6	6	0
Business Continuity Management	5	5	0
Information Security	15	15	0
Outsourcing Technology Services	4	4	0
Total	30	30	0

These procedures were agreed to with City management and designed based on standard IT related best practices. These procedures should be evaluated with the City's other risk mitigating procedures, which include; penetration monitoring, vulnerability assessments, internal audit procedures, internal control monitoring, and other tests.

Risk Ratings

🟩 **Functioning** controls are controls which are appropriately designed and no reportable exceptions were noted during our review procedures.

🟨 **Low risk** exceptions are one off in nature or could expose the City to minor financial or operational losses. These exceptions have both a low likelihood and impact.

🟧 **Moderate risk** exceptions are either reoccurring in nature or could expose the City to financial or operational losses. These exceptions have a combination of likelihood and impact ranging from moderate to high.

🟥 **High risk** exceptions require immediate corrective action and could expose the City to significant financial or operational losses. These exceptions have both a high impact and likelihood.

Based on the work performed and the risk rating scale, the overall rating for this review is considered:

🟩 **Satisfactory**

The specific procedures performed were based on the concept of selective testing. Had additional or expanded procedures been performed, other matters might have come to our attention that would have been reported to you.

It should also be recognized that internal controls are designed to provide reasonable, but not absolute assurance that errors and irregularities will not occur, and that City activities are performed in accordance with the intentions of City management. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal controls. In the performance of most internal control procedures, errors can result, and controls can be circumvented intentionally by management. Further, controls may become ineffective due to newly identified business or technology exposures. The projection of any evaluation of internal control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, and that the degree of compliance with procedures may deteriorate.

We would like to thank management and staff for their assistance and courtesy extended to us during the course of our review.

The following is a summary of the exceptions and observations noted during the review:

Exceptions

No exceptions were noted as a result of our procedures.

Observations

Business Continuity Management – Training
We noted the City's Master Continuity of Operations Plan (COOP) was finalized in February 2020, just before the outbreak of the COVID-19 pandemic in March 2020. Per discussions with management, continuity training was in the City's plans but has yet to take place due to the pandemic. We recommend management prioritize continuity training as soon as the circumstances of the pandemic permit the City to do so to ensure all employees are educated on the COOP and their role in a potential continuity scenario.

Information Security – Network Traffic and Port Monitoring
We noted while the IT Department has the ability to restrict access to the various ports and drives on City assets, the decision has been made not to do so due to the frequent need and use of such ports and drives across multiple departments. Per inquiry with IT Department management, we noted the department is aware of the potential risks associated with the use of ports and drives on City assets and considers the current monitoring structure sufficient to mitigate those risks.

Information Security – Logical Security: Remote Access
We noted certain employees are allowed email access on personal and City-issued cell phones, but there is not a process in place for monitoring the operating software of the devices which are granted access to City emails. There is a risk associated with out-of-date operating systems and missing security updates. Per inquiry with IT Department management, we noted Arctic Fox monitors the City's Office 365 activity 24/7 and alerts the department of any suspicious activity immediately. The department is aware of the potential risks associated with City email access on devices with out-of-date security updates but considers the current monitoring structure sufficient to mitigate those risks.

Management

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
IT Governance	IT governance consists of leadership and organizational structures and processes that ensure the City's IT sustains and extends the City's strategies and objectives. IT governance ensures that IT generates operational value for the City and mitigates risks posed by using technology.	Key	We obtained and reviewed the City's 5-Year Information Technology Strategy Refresh, which was developed in conjunction with an external consulting group in May 2019. We noted the Strategy identifies four core strategies which should be the focus of the City's IT initiatives over the 5-year horizon. A total of 12 initiaves covering the four strategies have been identified.	No exceptions noted.
IT Responsibilities and Functions	City management ensures development, implementation, and maintenance of an effective IT risk management structure.	Key	We inquired of management and reviewed the City's organizational chart, noting the City's IT Department is lead by Robert Mullis, IT Director. The IT Department reports to the Assistant City Manager who then reports to the City Manager. Generally, IT related decisions are made jointly by the City Manager, IT Director, and Finance Director.	No exceptions noted.
Information Systems Reporting	Information systems reporting is effective as a feedback tool for City management and staff and are timely, accurate, consistent, complete, and relevant.	Secondary	We inquired of management to gain an understanding of the IT department's process for monitoring activity within various IT related applications and reviewing periodic reports provided by the City's various third-party service providers.	No exceptions noted.

Management

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Risk Mitigation: Personnel	City management has implemented effective control and risk transfer practices, such as the hiring and training of personnel, as part of its overall IT risk mitigation strategy.	Secondary	We inquired of management and noted all new employees are required to sign the Employee Handbook and Policies Acknowledgement upon being hired. The policies covered include various information security related policies. Additionally, we noted the City has begun using KnowBe4 for periodic social engineering tests and related training. We obtained the signed form for a selection of employees hired within the past 12 months to verify new employees have been required to acknowledge the handbook and information security policies.	No exceptions noted.
Risk Mitigation: Insurance	City management has established an insurance program that is commensurate with the size, complexity, and risk of the City.	Secondary	We obtained and inspected the City's cyber liability insurance policy, which is effective through May 1, 2022, and noted the policy provides coverage for a variety of IT related events including ransomware attacks, cybersecurity event management and response, cyber extortion, and security/privacy liability.	No exceptions noted.

Management

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
IT Responsibilities and Functions: Human Resources	City management has considered appropriate succession and transition strategies for key managers and staff members.	Secondary	We reviewed the City's Organizational Chart to verify City management has established a reporting structure for the IT department. We inquired of IT department management to verify qualified personnel are available to take on additional responsibilities in the event the IT Director or another key member of the department is unable to perform their responsibilities.	No exceptions noted.

Business Continuity Management

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Policy and Procedures	Business Continuity Policy and procedures are up-to-date, reflective of the current business environment, and communicated throughout the entity.	Key	We obtained the City's Master Continuity of Operations Plan (COOP) and noted the purpose of the COOP is to ensure continuity of the City's essential functions under all threats and conditions, with or without warning. The COOP outlines ongoing preparedness activities for a successful response when the Plan has to be enacted.	No exceptions noted.
Risk Assessment	City management has adequately evaluated the likelihood and impact of potential disruptions and events.	Key	We reviewed the City's COOP and noted the City conducted an analysis and determined the threats and hazards that are most likely to impact operations at City Hall and within the City of Brookhaven. Potential threats were evaluated based on the likelihood of occurrence, the potential severity of the impact, and an overall ranking of the associated threats and hazards.	No exceptions noted.

Business Continuity Management

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Training	City management includes training as part of the business continuity program to educate staff on resilience, business continuity goals, City-wide objectives, policies, and individual personnel roles and responsibilities.	Key	Per review of the City's COOP, we noted management believes the success and effectiveness of the COOP is dependent upon each employee knowing their roles and responsibilities. Emergency Management (EM) will oversee the training of Brookhaven personnel on the COOP. Training should include conducting drills and exercises. Individual departments will also test their plans and backups systems regularly.	Observations noted.
Exercises and Tests	City management has provided appropriate exercises and tests to verify that business continuity procedures support business continuity objectives.	Key	Per review of the City's COOP, we noted testing strategies should include conducting drills and exercises when personnel will use the COOP in response to a mock incidents impacting mission essential functions. Individual departments will also test their plans and backups systems regularly. Per further review, we noted within four weeks of completion of a training or testing exercise, EM will ensure an After-Action Report and Improvement Plan (IP) of the exercise is completed. This provides participants with an understanding of what they did well and what can be done to improve their responses to COOP situations.	No exceptions noted.

Business Continuity Management

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Resilience: Data Backup and Replication	City management has adequate data backup and replication resilience strategies in place.	Secondary	We inquired of Robert Mullis, IT Director, and reviewed Veeam backup summary reports to verify the City has adequate processes to ensure resilient backup strategies are in place.	No exceptions noted.

Information Security

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Mitigating Interconnectivity Risk	City management maintains network and connectivity diagrams and data flow charts to ensure adequacy of layered controls and to facilitate more timely recovery and restoration of systems when incidents occur.	Secondary	We inspected the City's current Network Diagram to obtain an understanding of the physical network and evaluate the architecture for weaknesses.	No exceptions noted.
Inventory and Classification of Assets	City management inventories and classify assets, including hardware, software, information, and connections.	Secondary	We inquired of management to gain an understanding of the IT Department's procedures for monitoring assets. We observed a member of management access Desktop Central and demonstrate the various way IT Department personnel can inventory, monitor, and access the City's assets.	No exceptions noted.
Configuration Management	City management has a process in place for managing and controlling configurations of systems, applications and other technologies.	Key	The IT Department is primarily responsible for managing and controlling system and application configurations. Only members of the IT Department have administrative access on the systems the department uses. The City has a qualified IT Director who is ultimately responsible for ensuring systems are properly configured and monitored.	No exceptions noted.

Information Security

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Patch Management	City management has implemented automated patch management systems and software to ensure all network components are appropriately updated.	Key	We inquired of management to gain an understanding of the IT Department's procedures for monitoring and implementing patches on City assets. We noted patch scans are performed every 24 hours, and IT personnel access the results of the scans through Desktop Central. We observed a member of management access Desktop Central and demonstrate how IT personnel review, monitor, and implement necessary patches on the City's machines.	No exceptions noted.
Network Traffic and Port Monitoring	City management has a process in place for monitoring ports and network traffic to identify anomalous activity and unauthorized network connections.	Secondary	Management has contracted with Arctic Wolf for firewall, network, intrusion detection/prevention, and web monitoring services. Alerts are instantaneously sent to IT Department personnel and correlated with other monitored events to recognize potential threats and provide quick, proactive responses to any unwanted activity. We obtained and reviewed examples of weekly and monthly reports provided by Arctic Wolf to verify adequate monitoring of network traffic activity.	Observations noted.

Information Security

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Monitoring for Unauthorized Software	City management has a process in place to monitor for unauthorized software installations and has instituted controls that would restrict the ability for users to install unauthorized software.	Secondary	We inquired of management and noted only IT Department personnel have the ability to download and install software on most City machines. Some City employees are granted local administrator rights. The IT Department monitors all software installed on City owned machines through Desktop Central. We observed a member of management access Desktop Central and demonstrate the various ways the IT department can monitor downloaded software. We noted software can be monitored at a high level by reviewing all software across all devices or at a granular level by reviewing all software on a specific device.	No exceptions noted.

Information Security

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Assurance and Testing	City management's implemented information security program is operating securely and reaching intended goals by performing self-assessments and independent organizations performing penetration tests, vulnerability assessments, and audits. Results are reported to appropriate personnel and trigger appropriate, timely, and reliable escalation and response procedures.	Secondary	Management has contracted with Arctic Wolf for monthly external vulnerability scans and real-time penetration attempt monitoring. The City will also begin using Arctic Wolf's internal vulnerability scan offering in the coming months. We obtained the most recent Vulnerability Review, which was performed in August 2021, as well as examples of weekly and monthly activity summary reports provided by Arctic Wolf to verify procedures are in place for vulnerability and penetration monitoring and remediation.	No exceptions noted.
Logical Security: Remote Access	Management has developed policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner.	Secondary	We inquired of management to gain an understanding of the procedures for granting VPN access to City employees. We noted VPN access is only permitted on City-issued devices and requires dual authentication with both a password and token. We inquired of management to gain an understanding of the procedures for granting and monitoring email access on personal and City-issued cell phones.	Observations noted.

Information Security

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Firewalls	Firewalls are being used to enforce policies regarding acceptable traffic and to screen the internal network from directly receiving external traffic.	Key	We reviewed the City's network diagram to ensure firewalls are utilized as expected. We noted management has contracted with Arctic Wolf for firewall, network, intrusion detection/prevention, and web monitoring services. Activity is monitored 24/7, alerts are generated around the clock as needed, and periodic reports are provided to the IT Department on a weekly and monthly basis to summarize monitored activity. Switch and firewall backups are performed through Network Configuration Manager (NCM). We observed a member of management access the NCM portal to verify backups are up-to-date and successful.	No exceptions noted.
Anti-virus	Anti-virus software is installed on servers and desktops and are maintaining up-to-date virus definitions.	Key	FortiClient anti-virus monitoring software is downloaded locally on all City machines. Scans are routinely run on all machines to identify and remediate potential issues.	No exceptions noted.

Information Security

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Physical Security - Restricted Access	Management applies appropriate physical security controls to protect its premises and more sensitive areas, such as its data center(s).	Key	We inquired of management and noted only the City's IT Department staff members have keys to the City's server room. All contractors or third-party service providers who require access to the server room are accompanied by at least one of the IT Department staff members who have been issued a key.	No exceptions noted.
Physical Security - Environmental Controls	Detection devices, when applicable, are used to prevent theft and safeguard equipment from environmental threats.	Secondary	We inquired of management and noted the City's server room is outfitted with a fire extinguisher, uninterruptible power supply (UPS) devices, a backup generator, and a dedicated temperature control system with alerting capabilities.	No exceptions noted.
Network - Appropriate Access	User access to the network is appropriate and commensurate with job responsibilities.	Key	We inquired of management and noted initial employee access to the network is granted upon being hired as part of the employee onboarding process. The removal of employee rights is handled during the offboarding process through tickets in ZenDesk. Members of the IT Department are the only City employees with the ability to make these types of changes.	No exceptions noted.

Information Security

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Network - Privileged Access Controls	Privileged user access is restricted and activity is being adequately monitored.	Key	We inquired of management and noted IT Department personnel are the only employees with the ability to make changes to the network. Activity is logged by IT Department personnel in the Change Control Log within SharePoint.	No exceptions noted.
Network - Authentication and Access Restrictions	Network authentication and access restrictions are configured in accordance with policies and current industry standards.	Key	We reviewed the current security settings for the network and noted passwords for the network require various complexities and align with current industry standards.	No exceptions noted.

Outsourcing Technology Services

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Policy and Procedures	City management has developed and implemented an effective outsourcing oversight program which provides a framework for management to identify, measure, monitor, and control the risks associated with outsourcing.	Key	We obtained the City's Purchasing Policy and noted the Policy includes procedures for contract approval, required documentation for vendors, bidding procedures, evaluation procedures, ethical/professional standards and practices, etc.	No exceptions noted.
Risk Assessment	City management has a process in place to evaluate the quantity of risk at the inception of an outstanding decision by considering risks pertaining to the function outsourced, to the service provider, and to the technology used.	Key	Per review of the Purchasing Policy, we noted technical and commercial evaluations are performed in instances when the Contract Purchases / Professional Services purchasing method is required to be followed. Technical evaluations are performed by subject matter experts while commercial evaluations are performed by the Purchasing Department.	No exceptions noted.
Service Provider Selection	City management evaluates service provider proposals per the City's needs and performs due diligence on prospects.	Secondary	Per review of the Purchasing Policy, we noted City management has outlined the procedures to be followed when selecting a vendor or service provider based on a number of factors including the nature of the goods/services to be provided and the estimated cost of the purchase/contract.	No exceptions noted.

Outsourcing Technology Services

Control Title	Control Description	Control Type	Testing Performed by NCA	Exception(s) Risk Rating
Contracts	City management has a process in place to ensure contracts for outsourcing services with service providers contain adequate and measurable service level agreements, the rights and responsibilities of both parties, and required contract clauses addressing significant issues such as financial control and report, right to audit, ownership of data and programs, confidentiality, subcontractors and continuity of service.	Key	Per review of the Purchasing Policy, we noted a form of a contract will be executed or obtained for all vendor and service provider decisions. In situations where a formal contract is not required, a purchase order or similar document, approved by the appropriate level of management, is considered to be the contract.	No exceptions noted.