METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

METROPOLITAN NASHVILLE AUDIT COMMITTEE

WORKBOOK

April 12, 2022

Metropolitan Nashville
Audit Committee Meeting
Background Information for Audit Opinion

Charter Requirements

Sec. 6.15 the Charter states, "The council shall provide annually for an independent audit of the accounts and other evidences of financial transactions of the metropolitan government and of its every department, office and agency." Also in that same section, the Charter provides that "The council may at any time order an examination or special audit of any department, office or agency of the government."

Sec. 8.103(i) of the Charter which directs the Director of Finance to, "Prepare a complete annual report of the financial activities of all funds and all departments, boards, commissions, and agencies of the metropolitan government."

Governmental Accounting, Auditing, and Financial Reporting Standards and State Audit Manual

Currently, governmental accounting guidance gives governments two options regarding the combining statements. Metro will change from the opinion on the individual funds to the *in-relation-to opinion*; both are acceptable. The State Audit Manual provides the same option. Both are attached for reference. The auditors

Metro's Audit Opinion for FY21

Opinions

In our opinion, based on our audit and the reports of other auditors, the financial statements referred to above present fairly, in all material respects, the respective financial position of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of The Metropolitan Government of Nashville and Davidson County, Tennessee, as of June 30, 2021, and the respective changes in financial position and, where applicable, cash flows thereof, and the respective budgetary comparisons for the General Fund and the General Purpose School Fund for the year then ended in accordance with accounting principles generally accepted in the United States of America. In addition, in our opinion, based on our audit and the reports of other auditors, the financial statements referred to above present fairly, in all material respects, the respective financial position of each of the nonmajor governmental, nonmajor enterprise, internal service, and fiduciary funds, the Sports Authority Fund, the Industrial Development Board Fund, and each of the discretely presented component units as of June 30, 2021, and the respective changes in financial position and, where applicable, cash flows thereof for the year then ended in conformity with accounting principles generally accepted in the United States of America.

Other Information

Our audit was conducted for the purpose of forming opinions on the financial statements that collectively comprise the Government's basic financial statements, and each nonmajor governmental, nonmajor enterprise, internal service, and fiduciary funds, the Sports Authority Fund, the Industrial Development Board Fund, and the financial statements of each of the discreetly presented component units. The schedules on pages C-9, C-10, and C-11, and on pages G-2 through G-28, are presented for purposes of additional analysis and are not a required part of the basic financial statements.

Such information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the basic financial statements. Such information has been subjected to the auditing procedures applied in the audit of the basic financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic financial statements or to the basic financial statements themselves, and other additional procedures in accordance with auditing standards general accepted in the United States of America by us and other auditors. In our opinion, based on our audit, the procedures performed as described above, and the reports of the other auditors, in the information is fairly stated, in all material respects, in relation to the basic financial statements as a whole.

Metro's Audit Opinion for FY22

Opinions

In our opinion, based on our audit and the reports of other auditors, the financial statements referred to above present fairly, in all material respects, the respective financial position of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of The Metropolitan Government of Nashville and Davidson County, Tennessee, as of June 30, 2021, and the respective changes in financial position and, where applicable, cash flows thereof, and the respective budgetary comparisons for the General Fund and the General Purpose School Fund for the year then ended in accordance with accounting principles generally accepted in the United States of America. In addition, in our opinion, based on our audit and the reports of other auditors, the financial statements referred to above present fairly, in all material respects, the respective financial position of each of the Sports Authority Fund, the Industrial Development Board Fund, and each of the discretely presented component units as of June 30, 2021, and the respective changes in financial position and, where applicable, cash flows thereof for the year then ended in conformity with accounting principles generally accepted in the United States of America.

Other Information

Our audit was conducted for the purpose of forming opinions on the financial statements that collectively comprise the Government's basic financial statements, the Sports Authority Fund, the Industrial Development Board Fund, and the financial statements of each of the discreetly presented component units. The combining and individual fund statements, and the schedules on pages C-9, C-10, and C-11, and on pages G-2 through G-28, are presented for purposes of additional analysis and are not a required part of the basic financial statements.

Such information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the basic financial statements. Such information has been subjected to the auditing procedures applied in the audit of the basic financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic financial statements or to the basic financial statements themselves, and other additional procedures in accordance with auditing standards general accepted in the United States of America by us and other auditors. In our opinion, based on our audit, the procedures performed as described above, and the reports of the other auditors, in the information is fairly stated, in all material respects, in relation to the basic financial statements as a whole.

Tennessee Comptroller of the Treasury

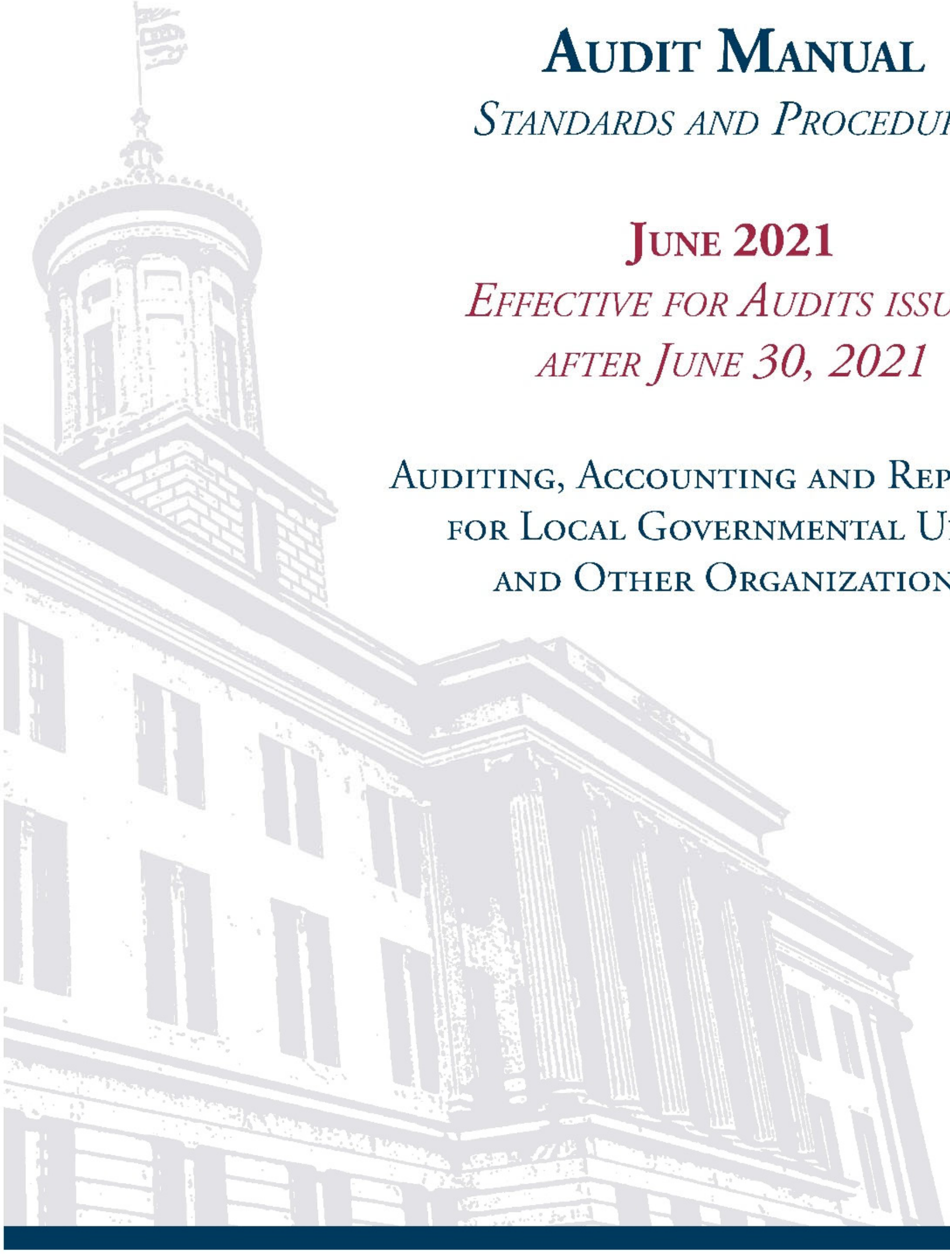
Audit Manual

Standards and Procedures

June 2021

Effective for Audits issued after June 30, 2021

Auditing, Accounting and Reporting for Local Governmental Units and Other Organizations



Jason E. Mumpower
Comptroller of the Treasury

Department of Audit

Those governmental units and recipients of subrecipient funding that are subject to any federal audit provisions must comply with those audit standards as well, which can be found at https://www.whitehouse.gov/omb/information-for-agencies/circulars/ .

The statutory and contractual audit and internal control requirements for different entities are summarized in the introduction of this manual. The internal control documentation requirements for various entities are addressed in the *Internal Control and Compliance Manual* released by the Comptroller's Office in December 2015. The provisions and documentation requirements of that manual should be considered when evaluating and reporting on internal control in accordance with the requirements of *Government Auditing Standards*.

If, during the course of the audit, it becomes apparent that a disclaimer of opinion or adverse opinion will likely be required, the auditor should contact the Division of Local Government Audit.

Coverage

The audit must generally cover all funds and all offices, departments, agencies, or other units of the entity that collect or disburse funds or provide services or supervise any other assets belonging to the entity. Separate audits may be conducted for one or more departments if deemed necessary by the governing body and if approved by the Tennessee Comptroller of the Treasury.

Program-specific audits must be approved prior to the execution of a Contract to Audit Accounts. ***Section H*** includes general guidance for program-specific audits. Variances from these guidelines must be approved by the Tennessee Comptroller of the Treasury.

For governmental agencies, the reporting entity should be determined in accordance with standards established by the Governmental Accounting Standards Board (GASB). For nongovernmental agencies, the parent and all subsidiaries are normally included in the scope of the audit. Audits of agencies whose audit requirement is driven by funding from the Department of Intellectual and Developmental Disabilities (DIDD) must include the parent and all subsidiaries. Audits of agencies whose audit requirement is NOT driven by funding from DIDD, may, if approved by the state funding agency and the Comptroller of the Treasury of the State of Tennessee prior to executing a Contract to Audit Accounts, have an audit that only includes a particular subsidiary.

The auditor must consider materiality for any local government as provided for in the AICPA Audit and Accounting Guide, *State and Local Governments*.

The Comptroller of the Treasury shall require auditors of local governments to express an opinion on each of the opinion units which collectively comprise the basic financial statements required by the GASB Statement 34 financial reporting model. However, except for internal school funds and noncentralized cafeteria funds, a local government, at its option, may engage the auditor to also express an opinion on the combining and individual fund financial statements that are presented as supplementary information accompanying the basic financial statements. The combining and individual fund financial statements for internal school funds and noncentralized cafeteria funds must be covered in the auditor's opinion on the financial statements.

FINAL REPORT

Audit of the Metro Public Health Department - Information Technology Security Management and Governance

April 1, 2022

A Report to the Audit Committee

Mayor
John Cooper

Chief Medical Director of Health
Dr. Gill Wright III, MD

Chief Administrative Director of Health
Tina Lester, RN, MSN

Audit Committee Members
Tom Bates
Kelly Flannery
Sharon Hurt
Brackney Reed
Jim Shulman
Kyonztè Toombs

Metropolitan Nashville Office of Internal Audit

AUDIT OF THE HEALTH DEPARTMENT – INFORMATION TECHNOLOGY SECURITY MANAGEMENT AND GOVERNANCE

EXECUTIVE SUMMARY

April 1, 2022

Why We Did This Audit

The audit was performed due to the importance of ensuring the mitigation of information technology, security, and governance risks through designed and implemented controls at the Metro Public Health Department.

What We Recommend

- Ensure logical and physical access is removed timely.
- Establish a process to perform periodic internal and external penetration testing.
- Perform and document a formal risk assessment related to security of information.
- Document formal testing programs for business continuity, disaster recovery, and incident response scenarios.
- Document a formal business impact analysis addressing threats and disruptions of services, systems, personnel, facilities, and third-party services.

BACKGROUND

The Metro Public Health Department's mission is to protect, improve, and sustain the well-being of all people in Metropolitan Nashville. The department operates on the core values of professionalism, respect, integrity, dedication, and equity.

OBJECTIVES AND SCOPE

KraftCPAs PLLC was retained to evaluate the design and effectiveness of the internal controls related to the Health Department for the period January 1, 2020, through April 30, 2021. Areas of audit emphasis included, but were not limited to:

- Controls around protected health information.
- Assessment and mitigation of threats and vulnerabilities.
- Policies and procedures for security incidents.
- Employee training on handling sensitive information.
- Maintenance of secure computing environments.
- System protection through phsyical, environmental, and logical security controls.

WHAT WE FOUND

The following table identifies the functional area tested where observations exist, along with the number of observations by risk level. Red reflects audit observations that are considered high risk, yellow reflects audit observations of medium risk, and green reflects observations of low risk.

Internal Audit Area	Auditor's Grade	High	Medium	Low	Page
User Access Removal and Review	Needs Improvement	1	-	-	6
Penetration Testing		-	1	-	7
Risk Assessment and Data Classification Policy Documentation		-	1	-	7
Inadequate Business Continuity and Incident Response Plan Testing Program		-	1	-	8
Insufficient Business Impact Analysis		-	1	-	9
Delayed New Hire Training		-		1	10
Informal Change Management Documentation		-	-	1	12
Visitor Logs		-	-	1	12
Total		**1**	**4**	**3**	

Chart page numbers refer to the KraftCPAs PLLC full report, Appendix A.

GOVERNMENT AUDITING STANDARDS COMPLIANCE

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

METHODOLOGY

To accomplish our audit objectives, we performed the following steps:

- KraftCPAs PLLC was hired to assist with this engagement.
- The detailed methodology employed by KraftCPAs PLLC can be found in **Appendix A.**

AUDIT TEAM

KraftCPAs PLLC

Scott Nalley, CPA, CIA, CISA, Member – Risk Assurance & Advisory Services

Erica Hightower, CPA, CISA, Manager – Risk Assurance & Advisory Services

Metropolitan Nashville Office of Internal Audit

Lauren Riley, CPA, CIA, CFE, ACDA, CMFO, Metropolitan Auditor

APPENDIX A – Report From KraftCPAs PLLC

KraftCPAs PLLC was hired to assist with this engagement. The firm issued a report to the Office of Internal Audit, with details on objectives, methodology, observations, and recommendations. The report begins on the next page.

Metropolitan Government of Nashville and Davidson County Health Department

Information Technology Security Management and Governance Audit

Integrated Audit Report

For the period
January 1, 2020 through April 30, 2021

KraftCPAs
PLLC

This audit was performed at the request of the Metropolitan Nashville Office of Internal Audit. As such, the Tennessee Open Records Act makes this report subject to public disclosure.

Metropolitan Government of Nashville and Davidson County

Health Department Information Technology Security Management and Governance Audit

Table of Contents

Report Distribution:

Name	**Title**
Dr. Gill Wright III, MD	Chief Medical Director of Health
Tina Lester, RN, MSN	Chief Administrative Director of Health
Jim Diamond	Bureau Director, Health Department
Tonya Hatten	Program Director, Records Management
John Griffey	Assistant Director, Information Technology Services

Additional Distribution:

Name	**Title**
Lauren Riley	Metropolitan Auditor

I. Executive Summary

Introduction

KraftCPAs PLLC performed certain internal audit services for The Metropolitan Government of Nashville and Davidson County Office of Internal Audit related to Health Department Information Technology Security Management and Governance. Our services were performed in accordance with contract number 433868 between The Metropolitan Government of Nashville and Davidson County (Metro) and KraftCPAs PLLC. We conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Scope and Objectives

Our primary objective was to evaluate the design and effectiveness of the internal controls related to the Health Department for the period January 1, 2020 through April 30, 2021. In accordance with the services provided, the Health Department processes and stores protected health information (PHI). In order to assess compliance with Health Insurance Portability and Accountability Act (HIPAA) requirements, the Health Department has engaged a third-party consultant to assist with the performance of a HIPAA Compliance Roadmap. This assessment was initiated in the fall of 2020 and according to Health Department personnel has not yet been completed due to consultant-imposed delays. Although our procedures were designed to gain assurance that the Health Department has designed and implemented controls to mitigate risks associated with information technology, information security, and data governance, compliance with HIPAA Privacy and Security Rules related to these objectives was also considered.

As such, areas of audit emphasis included, but were not limited to:

- Controls are in place to identify, classify, and secure sensitive data, including PHI;
- Departmental threats and vulnerabilities are assessed and mitigated through ongoing risk assessment activities;
- Policies and procedures are maintained to identify, contain, and recover from security incidents;
- Employees are trained on handling sensitive information, including PHI;
- Secure computing environments are maintained using network security tools and techniques (e.g., intrusion protection/prevention systems, firewalls);
- Physical, environmental, and logical security controls are in place to protect systems;
- Endpoint protections are used to protect systems (e.g., anti-virus, patching, change control);
- Monitoring is performed to track, alert, and analyze access to network resources and protected information;
- Vendor management procedures are in place to protect systems;

- Systems and processes are regularly tested and evaluated (e.g., internal/external scans, penetration testing, internal control assessments, etc.); and
- Business continuity and disaster recovery policies are maintained and tested.

In order to achieve our audit objectives, we performed the following procedures:

- Reviewed applicable laws and regulations;
- Gained an understanding of processes and controls in place during the audit period; and
- Tested controls implemented by the Health Department.

Testing procedures included the following:

Test	Description
Inspection	Inspected documents and reporting indicating performance of control activity.
Observation	Observed application of specific control activities.
Inquiry	Inquired with key personnel and corroborated responses with management.

II. Overview of Results

During the course of our work, we discussed potential observations with management. A summary of key issues is provided later in **Section III** along with our risk level assessment.

In order to enhance your understanding of each specific observation, we have provided a risk level, defined as follows:

High - Requires immediate management attention. This is a serious internal control or risk management issue that may, with a high degree of certainty, lead to substantial losses, serious reputation damage, or significant adverse impact.

Medium - Requires timely management attention. This is an internal control or risk management issue that may lead to financial losses, reputation damage, or adverse impact, such as public sanctions or immaterial fines.

Low - Routine management attention is warranted. This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the process being tested. Risks are limited.

Based on our procedures and assessment of the observations noted, we have provided an overall audit grade. The audit grade is not intended to usurp ultimate risk assessment responsibility, which is vested with the audit committee and management. Overall audit grades are defined as follows:

Satisfactory - Observations are limited to minor deviations from policy or regulatory requirements resulting in nominal risk to the organization. The design and operating effectiveness of controls evaluated during the audit appear adequate and reasonable.

However, because of inherent limitations in any system of internal control, errors or irregularities may occur and not be detected. Therefore, absolute reliance should not be placed on these controls.

Needs Improvement - Observations include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in reasonable probability of further misstatements or violations, if not corrected promptly. The design and operating effectiveness of controls evaluated during the audit appear to be less than adequate, and limited reliance can be placed on these controls.

Unsatisfactory - Observations include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in probable misstatements or violations that could be significantly detrimental. Immediate corrective action by high-level management will be desirable. Findings in this category will immediately be reported to the appropriate level to ensure timely action can be taken. The design and operating effectiveness of controls evaluated during the audit are not effective and should not be considered reliable.

III. Observations and Conclusion Summary

The following table identifies the functional area tested where observations exist, along with the number of observations by risk level. Red reflects audit observations that are considered high risk, yellow reflects audit observations of medium risk, and green reflects observations of low risk.

Internal Audit Area	Auditor's Grade	High	Medium	Low	Page
User Access Removal and Review	Needs Improvement	1	-	-	6
Penetration Testing		-	1	-	7
Risk Assessment and Data Classification Policy Documentation		-	1	-	7
Inadequate Business Continuity and Incident Response Plan Testing Program		-	1	-	8
Insufficient Business Impact Analysis		-	1	-	9
Delayed New Hire Training		-	-	1	10
Informal Change Management Documentation		-	-	1	12
Visitor Logs		-	-	1	12
Total		**1**	**4**	**3**	

<u>**Conclusion Summary**</u>

One High-risk issue was identified during our procedures, and our recommendations for the observations noted provide an opportunity to strengthen internal controls and processes. Our detailed observations and recommendations are described in **Section IV** of this report. Several of the findings and recommendations presented in this report may indicate a lack of due diligence expected to demonstrate compliance with HIPAA. Accordingly, we recommend that management seek legal advice regarding HIPAA regulatory requirements, as considered necessary.

We appreciate the cooperation extended to us by various personnel and are pleased to be of service. If there are any questions or comments regarding this report, please contact us. Contact information for the member and manager overseeing this work is presented below.

Scott Nalley, CPA, CIA, CISA
Member, Risk Assurance & Advisory Services
615-782-4252
snalley@kraftcpas.com

Erica Hightower, CPA, CISA
Manager, Risk Assurance & Advisory Services
615-915-6605
ehightower@kraftcpas.com

IV. Observations and Recommendations

Observation A: **User Access Removal and Access Review**
Risk Level: **High**

Logical and physical access for terminated employees is not always removed timely, and management has not established a formal process to perform periodic access reviews for Health Department systems or physical locations. During our review of network access within Active Directory and physical access to Health Department offices and clinics in July 2021, we identified two active user accounts assigned to employees who were terminated between December 2020 and March 2021.

In addition, although management performs a review of access within one of the systems used by the Health Department, access reviews for all other critical and sensitive Health Department applications and systems are not performed. Also, while all office locations are secured by badge reader and management performs informal reviews of physical access to one office location, this review is not documented, and reviews of physical access to other Health Department locations and clinics are not performed.

Risk: Failure to remove access for terminated employees increases the risk of inappropriate access to Health Department data, systems, and information, including PHI, along with increasing the risk of data breaches. In addition, users may have inappropriate or unnecessary logical or physical access rights, which could result in unauthorized access to PHI, increasing financial and reputational risks.

Recommendation: Health Department management, in coordination with Information Technology Services (ITS), should continue to use employee termination checklists to ensure all logical and physical access is removed timely and appropriately. In addition, management should establish a process to perform access reviews at least annually, which consider access privileges for access all Health Department systems and physical locations. All access reviews should be documented and retained.

Management's Response: The Health Department has established procedures for removal of access to terminated employees, but unfortunately two were missed during the unprecedented times of COVID, where in addition to the 500 MPHD employees, hundreds of temporary workers were onboarded and offboarded due to the department's response to COVID. The department has revisited its procedures and reiterated the importance of timely removal from all applications and systems. Further, the department has recently hired an information systems security analyst. A significant portion of that employee's job responsibilities will be to continually review policies and procedures surrounding information security as well as systems and physical location access.

Responsibility: Health Department

Implementation Date: Already Implemented

Observation B: **Penetration Testing**
Risk Level: **Medium**

Health Department systems are not subjected to penetration testing. Although Metro ITS performs limited vulnerability scanning and penetration testing related to the Metro network, the scope of these assessments do not always include Health Department systems. While not explicitly required by HIPAA, organizations often utilize penetration testing to enhance their overall compliance program and demonstrate due diligence.

Risk: Existing internal or external vulnerabilities may be exploited, resulting in system compromise or unauthorized disclose of PHI or other sensitive Health Department information.

Recommendation: Health Department management, with the assistance of ITS, should establish a process to perform periodic internal and external penetration testing of Health Department systems. The results from penetration testing should be reviewed by ITS and Health Department management, and issues identified should be formally tracked until resolved.

Management's Response: Health Department and ITS management will work together to evaluate the need to perform penetration testing, or other additional security and vulnerability assessments of Health Department systems, in consideration of HIPAA requirements and other cybersecurity best practices.

Responsibility: Health Department and ITS

Implementation Date: December 31, 2022

Observation C: **Risk Assessment and Data Classification Policy Documentation**
Risk Level: **Medium**

The Health Department does not maintain a formal, documented risk assessment related to security of information systems, or a documented data classification, as may be necessary to demonstrate compliance with HIPAA Privacy and Security rules. Although management has implemented controls to protect PHI stored within the Metro network, policy which identifies and classifies all types of data stored, where it is stored, or how it is protected has not been documented. In addition, management has engaged a third party to assist with the performance of a HIPAA Security Risk Analysis; however, the assessment is not performed annually and does not adequately address all information assets related to information technology, information security, or privacy.

Risk: Risks associated with the security and protection of PHI or other sensitive information may not be adequately identified and mitigated. As a result, PHI or other Health Department data could be compromised, resulting in non-compliance with HIPAA requirements, as well as fines or other penalties.

Recommendation: Health Department management should perform and document a formal risk assessment related to security of information systems which addresses all information assets. The risk assessment should identify specific risk/threat scenarios and should clearly align the impact and mitigating controls for each threat in order to assign an appropriate residual risk rating. In addition, management should document a data classification policy which identifies the types of data stored, where it is stored, how it is protected, and how/when it should be disposed of. The risk assessment and data classification policy should be reviewed at least annually or when significant changes to the environment occur.

Management's Response: Beginning in 2018, the Health Department worked with ITS to establish and launch a server that was strictly for use with PHI. That server has different security groups than the others on the Metro network and only two Health Department employees and two server administrators from ITS have the ability to request and make changes to who has access to the data within those security groups. Employees who have access to ePHI have been instructed to store data on this server.

Focal Point, Metro's contracted HIPAA compliance vendor, does perform an annual assessment of Health Department systems and controls. As with any audit, samples of different systems, policies, etc. are examined as part of each year's assessment.

MPHD has recently hired an information systems security analyst. As part of their job responsibilities, they will perform an assessment of all of the department's systems and risks associated with different threats/scenarios related to them, be tasked with creating an inventory of what data is stored where and to work with staff in identifying the different risk levels associated with that data. The Health Department has operated with data being either protected health information or not, and the department will look at all of the data and determine if other risk ratings are necessary.

Responsibility: Health Department

Implementation Date: December 31, 2022

Observation D: **Inadequate Business Continuity and Incident Response Plan Testing Program**
Risk Level: **Medium**

The Health Department has not documented a formal testing program or established a formal process to perform periodic testing of the Business Continuity, Disaster Recovery, or Incident Response Plans, which may be necessary to demonstrate compliance with HIPAA Security Rules over contingency planning.

Risk: Inadequate plan testing may result in systems or business processes not being fully considered and planned for in the event of an emergency. In addition, an incident may cause greater than anticipated harm and disruption to business operations, resulting in non-compliance with HIPAA requirements, fines or other penalties, and a decrease of public trust and confidence.

Recommendation: Health Department management should document a formal testing program to identify and test scenarios related to the Business Continuity, Disaster Recovery, and Incident Response Plans. The program should establish the following:

- Expectations for all functional Health Department divisions;
- Key roles and responsibilities of participants; and
- Expectations for planning testing scenarios and documenting, evaluating, and reporting test results.

In addition to documenting a formal testing program, the Health Department should establish a process to perform plan testing at least annually. Testing should include scenarios tested, roles and responsibilities, dates testing was performed, and the results and lessons learned from the exercise.

Management's Response: For the last two years, the Health Department has devoted a significant portion of our work to the real-life response to the COVID-19 pandemic. The pandemic has impacted and dictated nearly every facet of the department's work for the last two years. The department has shined in its response. No testing could have prepared the department for the challenges we have faced and continue to face each and every day as we try to protect the citizens and visitors of Davidson County. Despite the overwhelming need to dedicate significant numbers of staff to the pandemic response, all other Health Department activities have continued, even in the face of other providers of these services shutting down their operations.

The Health Department has had to onboard and offboard hundreds of temporary staff members as part of the response and the establishment of a mass vaccination operation, where over 100,000 vaccinations were given. All temporary staff was HIPAA trained prior to beginning their assignment. The Health Department will update the Continuity of Operations Plan and All Hazards Plan and consider the recommendations listed. The department's Multi-Year Training and Exercise Plan is an addendum to the All Hazards Plan and is scheduled to be updated this summer, pending the level of COVID operations between now and then.

Following the end of the COVID-19 operations, the Health Department will have a consultant-level after action report study done to examine the operations of the department during the pandemic. Any recommendations taken from that after action report will also be incorporated into those documents and will be updated periodically going forward.

Responsibility: Health Department

Implementation Date: December 31, 2022

Observation E: **Insufficient Business Impact Analysis**
Risk Level: **Medium**

The Health Department's Business Continuity and Disaster Recovery Plan does not currently include a Business Impact Analysis which defines specific recovery point objectives (RPOs) and recovery time objectives (RTOs) for critical Health Department systems.

Risk: Failure to document and maintain an adequate business impact analysis, including defined RPOs and RTOs, for critical Health Department systems may result in an incident causing greater than anticipated harm or disruption to business operations.

Recommendation: Health Department management should document a formal business impact analysis which addresses the impact and probability of specific threats and disruptions of services, systems, personnel, facilities, and services provided by third parties. The analysis should include disruptions related to natural events, technical events, malicious activity, and pandemics, and it should be reviewed at least annually or when significant changes to the environment occur.

Management's Response: As outlined in E above, the Health Department has been operating in a real-life pandemic response for the last two years. Lessons learned during the pandemic will inform the department of how best to respond to this or similar events in the future.

The department will incorporate a business impact analysis into the existing Continuity of Operations Plan and the All Hazards Plan. The Public Health Emergency Planning Team participates in a "Hazard Vulnerability Assessment" review every other year with local healthcare partners to identify and prioritize our threats (cyberattack, tornado, etc.). This is a grant requirement for PHEP, as it outlines our planning and exercise priorities.

Responsibility: Health Department

Implementation Date: December 31, 2022

Observation F: **Delayed New Hire Training**
Risk Level: **Low**

Health Department new hires do not always complete HIPAA and information security training timely upon hire. During our review of employees hired during the testing period, we identified three new hires, out of a sample of nine, who did not complete HIPAA or information security training within one month of hire. For these three employees, training occurred between 33 and 47 days after hire, and two of the identified employees were assigned job roles which typically have access to PHI in alignment with their duties.

It is the Health Department's current practice to provide orientation and training to new employees in groups, generally within one month of hire. However, the Health Department was unable to adhere to established training protocols throughout the testing period due to limited staffing caused by the Covid-19 pandemic. Although employees must acknowledge the Metro Acceptable Use of Information Assets Policy upon hire and prior to accessing Metro systems, this policy does not address HIPAA Privacy and Security requirements, nor does it adequately address best practice security standards to be used when accessing Health Department systems, including email or applications storing PHI. As a result, the Health Department's new hire training program may not have incorporated the due diligence necessary to demonstrate compliance with HIPAA Privacy and Security requirement during this time.

Risk: Health Department personnel may not be aware of their roles and responsibilities regarding HIPAA Privacy and Security requirements or general information security best practices. This increases the risk of unauthorized or unintentional disclosure of protected information and non-compliance with HIPAA requirements, which could result in fines or additional penalties.

Recommendation: Health Department management should establish a process to ensure that all new employees complete HIPAA Privacy and Security training within one month of hire. If training, is not performed within this period, access to PHI and other sensitive information should be restricted until training is completed.

Management's Response: MPHD hosts new employee orientation monthly, where all employees are given HIPAA training and sign off on receiving that training. The department feels that formal training within one month of hire fits HIPAA's "reasonable period of time" timeframe and provides each new hire with the training needed to protect the information entrusted to them. MPHD's monthly new hire orientation schedule is consistent with other Metro department training requirements as well as the guidance provided by several of Metro's HIPAA compliance vendors through the years, including Focal Point – the current vendor, that both stipulate new hire HIPAA training within 30 days of hire.

New employees are also trained in their specific work areas from day one of their employment and partnered with at least one experienced employee of the department. During this time, the new employee is trained on their specific job functions, including applicable programmatic procedures for handling of PHI/HIPAA information as well as accessing any systems or paper records that they will come into contact with as part of their job duties.

As noted, all new employees are required to read and sign an acknowledgement of reading and understanding Metro's Acceptable Use of Information Technology Assets Policy prior to being given access to Metro's network. While this policy may not name HIPAA specifically, it is pretty comprehensive in addressing the use and/or dissemination of sensitive information, data encryption, access to the network, access to secured areas, storage of information, and reporting of security incidents.

The samples reviewed by the auditors were pulled during COVID, so not all employees were on site to receive such training and trainings were not held monthly due to low numbers of available new staff. Further, some of the employees sampled were PRN School Health nurses, and school was not in session during this time. With no school and the PRN nurses working on an as-needed basis, they did not have access to any PHI at the time. The department has resumed monthly new employee orientation, and all new employees are given HIPAA training. Also, all department employees are required to take HIPAA training annually.

Responsibility: Health Department

Implementation Date: Already Implemented

Observation G: **Informal Change Management Documentation**
Risk Level: **Low**

The Health Department does not currently document or retain evidence of change control procedures followed, including testing or approval of application or other system changes prior to implementation, as required by the Metro Change Management Policy.

Risk: Informal or inconsistent documentation may result in insufficient deliverables, inefficient use of resources, or increased risk of system vulnerabilities.

Recommendation: Health Department management should ensure that supporting documentation is consistently maintained for all changes implemented. Documentation should include approvals, results of risk assessment activities and testing, and formal backout and communication plans, where applicable.

Management's Response: The department will keep records of all supporting documentation with regard to changes requested, approved, denied within the department for all applications. For items involving servers managed by ITS, the department will maintain the above plus any communications with ITS regarding implementation of the changes requested.

Responsibility: Health Department

Implementation Date: Already Implemented

Observation H: **Insufficient Visitor Logs**
Risk Level: **Low**

Health Department non-patient visitors (i.e., contractors or other third-parties) are not required to sign-in to a visitor log when entering and exiting secure locations. Although visitors are required to be escorted at all Health Department locations, a visitor log is not currently maintained, which may be necessary to demonstrate compliance with HIPAA Security Rules. In addition, visitors are not currently required to wear a visitor badge or other identifying feature.

Risk: Visitors may not be properly authenticated or tracked, resulting in unauthorized access to PHI or other sensitive Health Department information. In addition, failing to document visitors increases the risk of non-compliance with HIPAA requirements, which could result in fines or penalties.

Recommendation: Health Department management should implement the use of visitor logs at all office locations and clinics to track non-patient visitors, including visitor names, associated organization, purpose of visitation, assigned escort, and entry/exit times. In addition, management should implement the use of visitor badges or other method to easily identify visitors while on-site.

Management's Response: Vendors who do business with Metro have contracts that include business associate agreements that are structured to cover both Metro and the vendor with regard to protecting PHI and/or other HIPAA-related information. If these vendors have access to be in secured areas, they are issued ID badges that allow them into these areas and their entrance to these areas are logged when the badges are used on the card readers.

As mentioned in the observation, all visitors who are in secured areas are required to be escorted by an MPHD staff member at all times per Health Department policy. Health Department employees are all HIPAA trained and all aware of their responsibilities under HIPAA to not allow visitors access to PHI while they are escorting visitors in secured areas. Also, Health Department employees lock their computers when away from them to prevent any unauthorized viewing of their monitors. Any paper records that contain PHI are locked away in files when not in use as well.

The Health Department's main building, the Lentz Public Health Center, is operated by Metro's General Services Department, so the Health Department will begin conversations with General Services to determine if visitor logs and/or visitor badges are necessary and appropriate given the safeguards already in place and in practice by the Health Department in observance of HIPAA Security Rules. The use and maintenance of visitor logs and badges could require financial commitments in terms of additional staffing that are not currently budgeted.

Responsibility: Health Department

Implementation Date: July 1, 2022

APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN

We believe that operational management is in a unique position to best understand their operations and may be able to identify more innovative and effective approaches and we encourage them to do so when providing their response to our recommendations.

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
	Recommendations for management of the Health Department to:		
H	**A.** Health Department management, in coordination with Information Technology Services (ITS), should continue to use employee termination checklists to ensure all logical and physical access is removed timely and appropriately. In addition, management should establish a process to perform access reviews at least annually, which consider access privileges for access all Health Department systems and physical locations. All access reviews should be documented and retained.	**Accept**: The Health Department has established procedures for removal of access to terminated employees, but unfortunately two were missed during the unprecedented times of COVID, where in addition to the 500 MPHD employees, hundreds of temporary workers were onboarded and offboarded due to the department's response to COVID. The department has revisited its procedures and reiterated the importance of timely removal from all applications and systems. Further, the department has recently hired an information systems security analyst. A significant portion of that employee's job responsibilities will be to continually review policies and procedures surrounding information security as well as systems and physical location access.	**Already Implemented**
M	**B.** Health Department Management, with the assistance of ITS, should establish a process to perform periodic internal and external penetration testing of Health Department Systems. The results from penetration testing should be reviewed by ITS and Health Department Management, and issues identified should be formally tracked until resolved.	**Accept**: Health Department and ITS management will work together to evaluate the need to perform penetration testing, or other additional security and vulnerability assessments of Health Department systems, in consideration of HIPAA requirements and other cybersecurity best practices.	**December 31, 2022**
M	**C.** Health Department management should perform and document a formal risk assessment related to security of information systems which addresses all information assets. The risk assessment should identify specific risk/threat scenarios and should clearly align the impact and mitigating controls	**Accept**: Beginning in 2018, the Health Department worked with ITS to establish and launch a server that was strictly for use with PHI. That server has different security groups than the others on the Metro network and only two Health Department employees and two	**December 31, 2022**

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
	for each threat in order to assign an appropriate residual risk rating. In addition, management should document a data classification policy which identifies the types of data stored, where it is stored, how it is protected, and how/when it should be disposed of. The risk assessment and data classification policy should be reviewed at least annually or when significant changes to the environment occur.	server administrators from ITS have the ability to request and make changes to who has access to the data within those security groups. Employees who have access to ePHI have been instructed to store data on this server. Focal Point, Metro's contracted HIPAA compliance vendor, does perform an annual assessment of Health Department systems and controls. As with any audit, samples of different systems, policies, etc. are examined as part of each year's assessment. MPHD has recently hired an information systems security analyst. As part of their job responsibilities, they will perform an assessment of all of the department's systems and risks associated with different threats/scenarios related to them, be tasked with creating an inventory of what data is stored where and to work with staff in identifying the different risk levels associated with that data. The Health Department has operated with data being either protected health information or not, and the department will look at all of the data and determine if other risk ratings are necessary.	
M	**D.** Health Department management should document a formal testing program to identify and test scenarios related to the Business Continuity, Disaster Recovery, and Incident Response Plans. The program should establish the following: • Expectations for all functional Health Department divisions; • Key roles and responsibilities of participants; and • Expectations for planning testing	**Accept**: For the last two years, the Health Department has devoted a significant portion of our work to the real-life response to the COVID-19 pandemic. The pandemic has impacted and dictated nearly every facet of the department's work for the last two years. The department has shined in its response. No testing could have prepared the department for the challenges we have faced and continue to face each and every day	**December 31, 2022**

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
	scenarios and documenting, evaluating, and reporting test results. In addition to documenting a formal testing program, the Health Department should establish a process to perform plan testing at least annually. Testing should include scenarios tested, roles and responsibilities, dates testing was performed, and the results and lessons learned from the exercise.	as we try to protect the citizens and visitors of Davidson County. Despite the overwhelming need to dedicate significant numbers of staff to the pandemic response, all other Health Department activities have continued, even in the face of other providers of these services shutting down their operations. The Health Department has had to onboard and offboard hundreds of temporary staff members as part of the response and the establishment of a mass vaccination operation, where over 100,000 vaccinations were given. All temporary staff was HIPAA trained prior to beginning their assignment. The Health Department will update the Continuity of Operations Plan and All Hazards Plan and consider the recommendations listed. The department's Multi-Year Training and Exercise Plan is an addendum to the All Hazards Plan and is scheduled to be updated this summer, pending the level of COVID operations between now and then. Following the end of the COVID-19 operations, the Health Department will have a consultant-level after action report study done to examine the operations of the department during the pandemic. Any recommendations taken from that after action report will also be incorporated into those documents and will be updated periodically going forward.	
M	**E.** Health Department management should document a formal business impact analysis which addresses the impact and probability of specific threats and disruptions of services,	**Accept**: As outlined in E above, the Health Department has been operating in a real-life pandemic response for the last two years. Lessons learned during the pandemic	**December 31, 2022**

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
🟨	systems, personnel, facilities, and services provided by third parties. The analysis should include disruptions related to natural events, technical events, malicious activity, and pandemics, and it should be reviewed at least annually or when significant changes to the environment occur.	will inform the department of how best to respond to this or similar events in the future. The department will incorporate a business impact analysis into the existing Continuity of Operations Plan and the All Hazards Plan. The Public Health Emergency Planning Team participates in a "Hazard Vulnerability Assessment" review every other year with local healthcare partners to identify and prioritize our threats (cyberattack, tornado, etc.). This is a grant requirement for PHEP, as it outlines our planning and exercise priorities.	
L	**F.** Health Department management should establish a process to ensure that all new employees complete HIPAA Privacy and Security training within one month of hire. If training, is not performed within this period, access to PHI and other sensitive information should be restricted until training is completed.	**Accept**: MPHD hosts new employee orientation monthly, where all employees are given HIPAA training and sign off on receiving that training. The department feels that formal training within one month of hire fits HIPAA's "reasonable period of time" timeframe and provides each new hire with the training needed to protect the information entrusted to them. MPHD's monthly new hire orientation schedule is consistent with other Metro department training requirements as well as the guidance provided by several of Metro's HIPAA compliance vendors through the years, including Focal Point – the current vendor, that both stipulate new hire HIPAA training within 30 days of hire. New employees are also trained in their specific work areas from day one of their employment and partnered with at least one experienced employee of the department. During this time, the new employee is trained on their specific job functions, including	**Already Implemented**

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
🟩		applicable programmatic procedures for handling of PHI/HIPAA information as well as accessing any systems or paper records that they will come into contact with as part of their job duties. As noted, all new employees are required to read and sign an acknowledgement of reading and understanding Metro's Acceptable Use of Information Technology Assets Policy prior to being given access to Metro's network. While this policy may not name HIPAA specifically, it is pretty comprehensive in addressing the use and/or dissemination of sensitive information, data encryption, access to the network, access to secured areas, storage of information, and reporting of security incidents. The samples reviewed by the auditors were pulled during COVID, so not all employees were on site to receive such training and trainings were not held monthly due to low numbers of available new staff. Further, some of the employees sampled were PRN School Health nurses, and school was not in session during this time. With no school and the PRN nurses working on an as-needed basis, they did not have access to any PHI at the time. The department has resumed monthly new employee orientation, and all new employees are given HIPAA training. Also, all department employees are required to take HIPAA training annually.	

APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
L	**G**. Health Department management should ensure that supporting documentation is consistently maintained for all changes implemented. Documentation should include approvals, results of risk assessment activities and testing, and formal backout and communication plans, where applicable.	**Accept:** The department will keep records of all supporting documentation with regard to changes requested, approved, denied within the department for all applications. For items involving servers managed by ITS, the department will maintain the above plus any communications with ITS regarding implementation of the changes requested.	**Already Implemented**
L	**H.** Health Department management should implement the use of visitor logs at all office locations and clinics to track non-patient visitors, including visitor names, associated organization, purpose of visitation, assigned escort, and entry/exit times. In addition, management should implement the use of visitor badges or other method to easily identify visitors while on-site.	**Accept**: Vendors who do business with Metro have contracts that include business associate agreements that are structured to cover both Metro and the vendor with regard to protecting PHI and/or other HIPAA-related information. If these vendors have access to be in secured areas, they are issued ID badges that allow them into these areas and their entrance to these areas are logged when the badges are used on the card readers. As mentioned in the observation, all visitors who are in secured areas are required to be escorted by an MPHD staff member at all times per Health Department policy. Health Department employees are all HIPAA trained and all aware of their responsibilities under HIPAA to not allow visitors access to PHI while they are escorting visitors in secured areas. Also, Health Department employees lock their computers when away from them to prevent any unauthorized viewing of their monitors. Any paper records that contain PHI are locked away in files when not in use as well. The Health Department's main building, the Lentz Public Health Center, is operated by Metro's	**July 1, 2022**

	Recommendations	Concurrence and Action Plan	Proposed Completion Date
🟩		General Services Department, so the Health Department will begin conversations with General Services to determine if visitor logs and/or visitor badges are necessary and appropriate given the safeguards already in place and in practice by the Health Department in observance of HIPAA Security Rules. The use and maintenance of visitor logs and badges could require financial commitments in terms of additional staffing that are not currently budgeted.	

External Quality Control Review

of the

Metropolitan Government of Nashville and Davidson County

Conducted in accordance with guidelines of the

Association of Local Government Auditors

for the period January 1, 2019, through December 31, 2021

Association of Local Government Auditors

March 3, 2022

Ms. Lauren Riley
Metropolitan Auditor
404 James Robertson Parkway, Suite 190
Nashville, TN
37219-6300

Dear Ms. Lauren Riley,

We have completed a peer review of the Metropolitan Government of Nashville and Davidson County for the period January 1, 2019, through December 31, 2021. In accordance with generally accepted government auditing standards peer review requirements, we followed the standards and guidelines contained in the *Peer Review Guide* published by the Association of Local Government Auditors (ALGA).

We reviewed the internal quality control system of your audit organization and conducted tests in order to determine whether your internal quality control system was adequately designed and operating effectively to provide reasonable assurance of compliance with *Government Auditing Standards* issued by the Comptroller General of the United States and applicable legal and regulatory requirements. Our procedures included:

- Reviewing the audit organization's written policies and procedures.
- Reviewing internal monitoring procedures.
- Reviewing a sample of audit and attestation engagements and working papers.
- Reviewing documents related to independence, training, and development of auditing staff.
- Interviewing auditing staff, management, and members of the Audit Committee to assess their understanding of, and compliance with, relevant quality control policies and procedures.

Due to variances in individual performance and judgment, compliance does not imply adherence to standards in every case but does imply adherence in most situations. Organizations can receive a rating of pass, pass with deficiencies, or fail. The Metropolitan Government of Nashville and Davidson County has received a rating of pass.

Further, based on the results of our review, it is our opinion that the Metropolitan Government of Nashville and Davidson County's internal quality control system was adequately designed and operating effectively to provide reasonable assurance of compliance with *Government Auditing Standards* and applicable legal and regulatory requirements for audits during January 1, 2019, through December 31, 2021.

We extend our thanks to you, your staff, and the other officials we met for the hospitality and cooperation extended to us during our review.

Amanda Noble

Amanda Noble, CIA, CISA
City Auditor's Office
Atlanta, GA

Kasey Sawyer

Kasey Sawyer, CIA
Virginia Beach City Public Schools
Office of Internal Audit
Virginia Beach, VA

Lauren Riley
Metropolitan Auditor

OFFICE OF INTERNAL AUDIT
404 James Robertson Parkway, Suite 190
NASHVILLE, TENNESSEE 37201
615-862-6111

METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

March 3, 2022

Ms. Amanda Noble, CIA, CISA
City Auditor
Atlanta, GA

Ms. Kasey Sawyer, CIA
Internal Auditor
Virginia Beach City Public Schools

Dear Peer Review Team:

Subject: Metropolitan Nashville Office of Internal Audit External Quality Control Review

Thank you for performing the Metropolitan Nashville Office of Internal Audit external quality control review for the period January 1, 2019, through December 31, 2021. We appreciate your opinion that our audit quality control system complied with *Government Auditing Standards*. We also value the suggestions that you provided to help us excel and improve the quality of our audit process.

It was a pleasure working with a knowledgeable and skilled review team during this external quality control review.

Sincerely,

Lauren Riley

Lauren Riley

cc: Metropolitan Nashville Audit Committee

FINAL AUDIT REPORT

Audit Recommendations Follow-up – Audit of Metropolitan Nashville General Government Benefits

April 8, 2022

A Report to the Audit Committee

Mayor
John Cooper

Human Resources Director
Shannon Hall

Audit Committee Members
Tom Bates
Kelly Flannery
Sharon Hurt
Brackney Reed
Jim Shulman
Kyonztè Toombs

Metropolitan
Nashville
Office of
Internal Audit

Audit Recommendations Follow-Up - Audit of the Metropolitan Nashville General Government Benefits

EXECUTIVE SUMMARY

April 8, 2022

Why We Did This Audit

To evaluate management's implementation of previous audit recommendations as of March 1, 2022.

What We Recommend

Management should continue efforts to implement the one remaining recommendation.

BACKGROUND

On October 16, 2019, the Metropolitan Nashville Office of Internal Audit issued an audit report on Metropolitan Nashville General Government Benefits. The audit scope for this engagement was between July 1, 2016, and October 31, 2018. The audit report included four recommendations. Three recommendations were for the Department of Human Resources. One recommendation was for Metropolitan Nashville Public Schools. All recommendations were accepted by management. Office of Internal Audit guidelines require monitoring and follow-up to ensure that the recommendations assessed as high or medium risk are appropriately considered, effectively implemented, and yield intended results.

OBJECTIVES AND SCOPE

The objectives of this follow-up audit were to determine if the recommended action or an acceptable alternative was implemented.

The scope of the follow-up audit included all four accepted recommendations that management reported as implemented.

WHAT WE FOUND

The Department of Human Resources has fully implemented three recommendations, and Metropolitan Nashville Public Schools have partially implemented one recommendation with full implementation expected by June 1, 2022. Details of the implementation status can be seen in **Appendix A**.

AUDIT FOLLOW-UP RESULTS

The initial audit report encompassed the processes for initiating, monitoring, and terminating benefits for Metropolitan Nashville employees and included transactions between July 1, 2016, and October 31, 2018. The audit report included four recommendations all of which were accepted by management for implementation.

The Office of Internal Audit will close a recommendation only for one of the following reasons:

- The recommendation was effectively implemented.
- An alternative action was taken that achieved the intended results.
- Circumstances have so changed that the recommendation is no longer valid.
- The recommendation was not implemented despite the use of all feasible strategies or due to lack of resources. When a recommendation is closed for these reasons, a judgment is made on whether the objectives are significant enough to be pursued later in another assignment.

The scope of the follow-up audit included all four accepted recommendations that management reported as implemented. Of the four accepted recommendations, three recommendations were fully implemented, and one recommendation was partially implemented. Details of the implementation status and updated implementation dates, if applicable, can be seen in **Appendix A.**

METHODOLOGY

To achieve the audit objectives, auditors performed the following steps:

- Confirmed Dependent Eligibility Verification review.
- Reviewed Cigna and BlueCross BlueShield Claims Transactional and Operational Review Presentations to the Metropolitan Employee Benefit Board.
- Reviewed the Medical Plan Update Presentation to the Metropolitan Employee Benefit Board.
- Reviewed process narrative for the joint Human Resources and Payroll Division process for terminating a pension.
- Made inquiries into efforts made to better utilize Oracle R12 in improving payroll data collection from Metropolitan Nashville Charter Schools.
- Gained an understanding of the current process in place for obtaining payroll data from Metropolitan Nashville Charter Schools.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

AUDIT TEAM

Seth Hatfield, CPA, CIA, CFE, In-Charge Auditor

Bill Walker, CPA, CIA, CFE, Audit Manager

Lauren Riley, CPA, CIA, CFE, ACDA, CMFO, Metropolitan Auditor

APPENDIX A – PRIOR RECOMMENDATIONS AND IMPLEMENTATION STATUS

The following table shows the guidelines followed to determine the status of implementation.

Table 1

Recommendation Implementation Status	
Implemented / Closed	The department or agency provided sufficient and appropriate evidence to support the implementation of all elements of the recommendation and the recommendation's implementation caused or significantly influenced the benefits achieved.
Partially Implemented / Open	The department or agency provided some evidence to support implementation progress but not of all elements of the recommendation were implemented.
Not Implemented or No Longer Implemented	The department or agency did not implement a recommendation because: a) of lack of resources; b) an alternative action was taken that achieved the intended results; c) circumstances have so changed that the recommendation is no longer valid.

The following are the audit recommendations for the Human Resources Department made in our original audit report dated October 16, 2019, and the current implementation status of each recommendation based on our review of information and documents provided by the Human Resources Department.

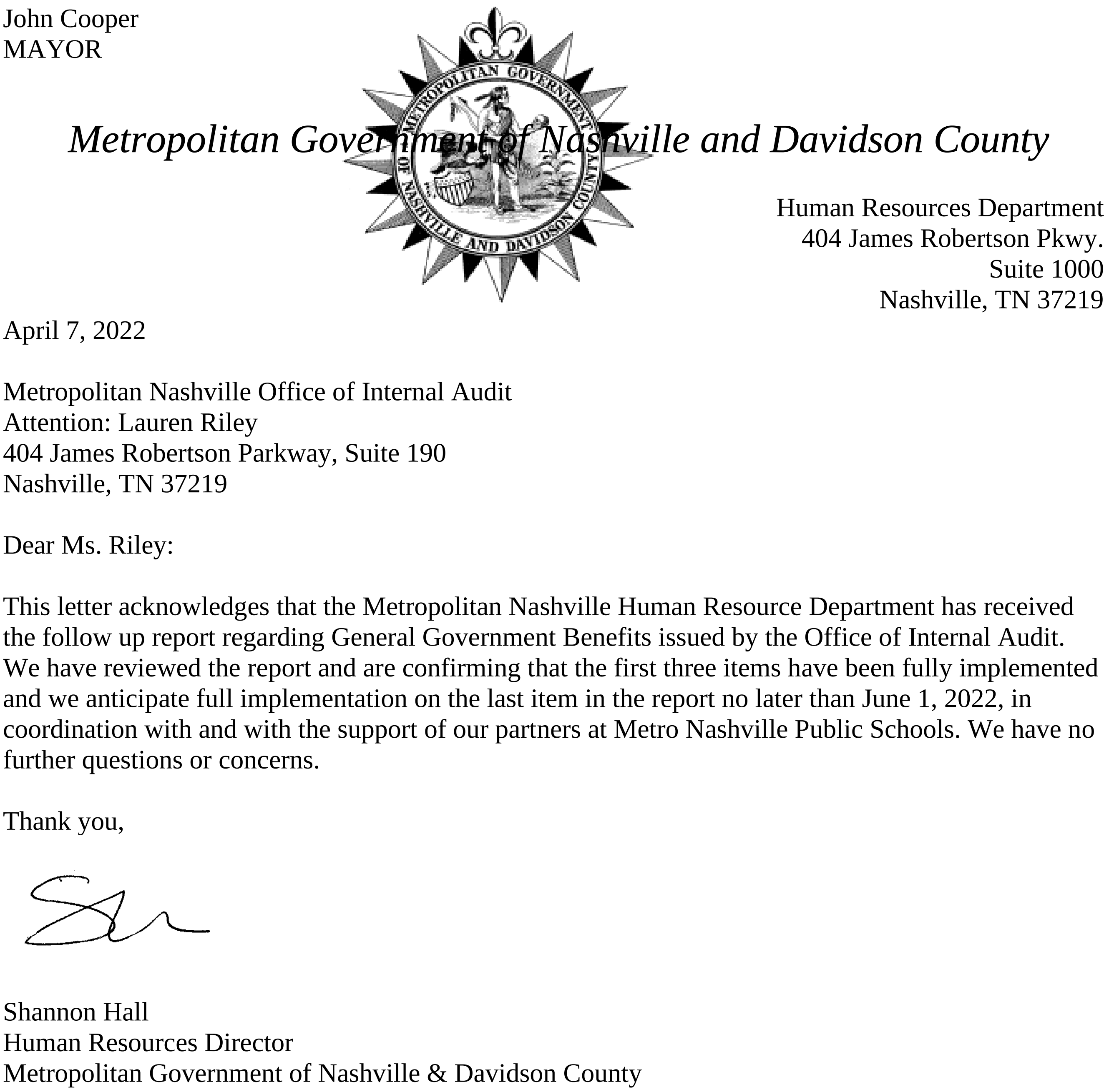
Recommendation	Implementation Actions	Outstanding Issues	Implementation Status
A.1 Conduct a dependent eligibility verification audit every five years. **Assessed Risk Level:** **Medium**	A dependent eligibility audit was conducted by Deloitte in 2021. These audits will be conducted every five years.	None	**Fully Implemented/ Closed**
A.2 Conduct an audit of insurance claims processed by insurance carriers on a triennial basis. **Assessed Risk Level:** **Medium**	A review of BlueCross BlueShield and Cigna claims was conducted by Deloitte. These reviews will be conducted triennially.	None	**Fully Implemented/ Closed**
C.1 Establish an extra layer of review when a pension benefit transfers to a survivor to ensure that the deceased pensioner's benefit stops on the correct date and the survivor's pension benefit begins on the correct date and no overlap occurs. **Assessed Risk Level**: **Medium**	The new process for terminating pensions is conducted jointly by the Human Resources Department and the payroll division within the Finance Department. The process narrative was reviewed by the Office of Internal Audit.	None	**Fully Implemented/ Closed**

APPENDIX A – PRIOR RECOMMENDATIONS AND IMPLEMENTATION STATUS

The following is the audit recommendation for Metropolitan Nashville Public Schools made in our original audit report dated October 16, 2019, and the current implementation status of the recommendation based on our review of information and documents provided by the Metropolitan Nashville Public Schools.

Recommendation	Implementation Actions	Outstanding Issues	Implementation Status
B.1 Explore the possibility of having charter schools' human resources and payroll systems interface with Oracle R12 to ensure that accurate benefits and pension information is communicated to the Metropolitan Nashville Human Resources Department. **Assessed Risk Level:** **High**	While the process for obtaining payroll information from Charter Schools is still manual, Metropolitan Nashville Schools has begun the process for using Oracle R12 to better collect payroll information from Charter Schools. The Director of Benefits stated that not all Charter Schools have been able to comply with the formatting necessary to utilize the export / import function in Oracle R12, but the department is still actively working on a solution for an integrated and automated method to collect pay information from Charter Schools. The Director of Human Resources stated this process is expected to go live in May 2022.	**Full implementation is expected to be completed by June 1, 2022.**	**Partially Implemented/ Open**

APPENDIX A – PRIOR RECOMMENDATIONS AND IMPLEMENTATION STATUS



John Cooper
MAYOR

Metropolitan Government of Nashville and Davidson County

Human Resources Department
404 James Robertson Pkwy.
Suite 1000
Nashville, TN 37219

April 7, 2022

Metropolitan Nashville Office of Internal Audit
Attention: Lauren Riley
404 James Robertson Parkway, Suite 190
Nashville, TN 37219

Dear Ms. Riley:

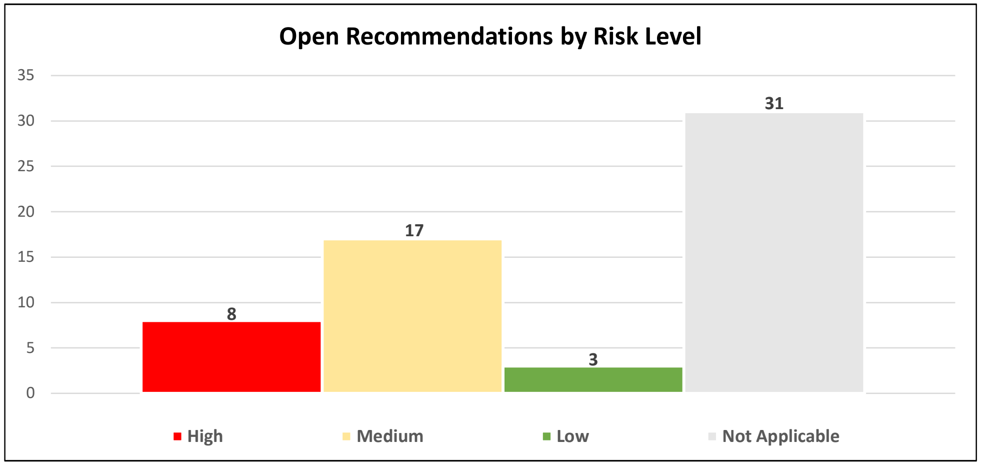
This letter acknowledges that the Metropolitan Nashville Human Resource Department has received the follow up report regarding General Government Benefits issued by the Office of Internal Audit. We have reviewed the report and are confirming that the first three items have been fully implemented and we anticipate full implementation on the last item in the report no later than June 1, 2022, in coordination with and with the support of our partners at Metro Nashville Public Schools. We have no further questions or concerns.

Thank you,

Shannon Hall
Human Resources Director
Metropolitan Government of Nashville & Davidson County

Implementation Status Update as of March 31, 2022

Audit Department List	Year	# Accepted	Open Recommendations Before Follow-Up	Implementation Due by 3/31/2022	Open Recs After Response	Notes
Assessor's Office	2014	14	3		3	
Historic Zoning and Historical Commission Work Force	2015	7	1		1	
Parks and Recreation Maintenance Division	2015	2.5	1		1	
General Government Occupational Safety Program	2017	24	23		23	
Finance Department Procurement And Business Assistance Office	2018	13	1		1	
Metro Water Services Fire Hydrant Inspections	2018	10	2		2	
Municipal Auditorium	2019	6	4		4	
NGH Pharmacy Operations	2019	17	1		1	
Election Commission Information Systems	2020	8	1		1	
Criminal Justice Center Project	2020	5	1		1	
State Trial Courts Drug Court 4	2020	16	1		1	
Trustee	2021	7	1		1	
Metro Water Services Billing Process	2021	2	1		1	
Fund Commitments, Restrictions, and Assignments	2021	2	1		1	
Public Defender's Office	2021	3	3		3	
Property Standards Complaints Process	2021	8	1		1	
Pension Investments	2021	6	6		6	
Public Works Revenue Collections	2021	16	2		2	
Health Department IT Audit	2022	8	8		5	
			62		59	



Metropolitan Nashville Office of Internal Audit
Audit Project Status
As of April 8, 2022

Audit Plan Year February 2022 to January 2023				**Report Phase**	
Projects	**Planning**	**Fieldwork**	**Report**	**Draft**	**Final**
1) MWS Collections		✓			
2) Barnes Fund			✓	Mar-22	
3) General Government Benefits Follow Up					Apr-22
4) Nashville General Hospital Human Resources	✓				
5) Agricultural Extension		✓			
6) Open Records Requests	✓				
7) Social Services Homelessness Impact Division	✓				
8) Health Department IT Security and Governance *(Kraft CPAs)*					Mar-22
9) MNPS Procurement Process			✓	Nov-21	
10) Office of Internal Audit - Peer Review		✓			Apr-22
11) Beer Board Follow Up					
Completed Investigations					**Final**
Metro Integrity Line Alerts - February 2022 to January 2023			**Total**	**Closed**	**Pending**
Metro Hotline Alerts (Fraud, Waste, & Abuse)			8	5	3

Note: Goal to complete 17 audit projects for Plan Year 2022. Currently 3 completed audit projects and 2 projects in the draft phase.

Metropolitan Nashville Office of Internal Audit
2022 Recommended Work Plan

***Co-source**	**CY 2021 Audits in Progress**	**Hours**
1	Barnes Fund Operations and Follow-Up	Draft Report
2	Metro Water Services Water and Sewer Collections	Fieldwork
3	Agricultural Extension Service	Fieldwork
4	Nashville General Hospital Human Resources Process	Planning
5	Metro Nashville Public Schools Procurement	Draft Report
6	Open Records Request Fulfillment Process	Planning
7	Social Services – Homelessness Impact Division	Planning
8	Health Department – Information Technology Security Management and Governance	Completed
	CY 2022 New Audit Areas	
9	NDOT Parking Management (*Carry Forward)*	
10	Office of Internal Audit Peer Review *(Carry Forward)*	Completed
11	Coronavirus Relief Funds Spending Process (*Carry Forward)*	
12	Metropolitan Council Staff	
13	Sports Authority / General Services - MLS Soccer Stadium Construction Project	
14	Metro Human Resources New Hire / Promotions On-Boarding Process	
15	Metro Nashville Police Department Early Intervention	
16*	Metro Nashville Disaster Recovery Planning Process	
17	License Plate Readers Pilot Program	
18	Criminal Court Clerk	
19	Sheriff's Office Locally Sentenced Felons Cost Settlement	
20	MNPS Building Accessibility and Security	
	Information Technology Risk	
21	Community Development and Regulation Implementation Project	
22*	PCI-DSS Compliance Assessment	
	Audit Recommendation Follow-up	
23	Recommendation Implementation Follow-Up Audits	
	Other 2022 Audit Services Effort	
	Investigation Services	In Process
	Special Projects	
	Unforeseen Requests	

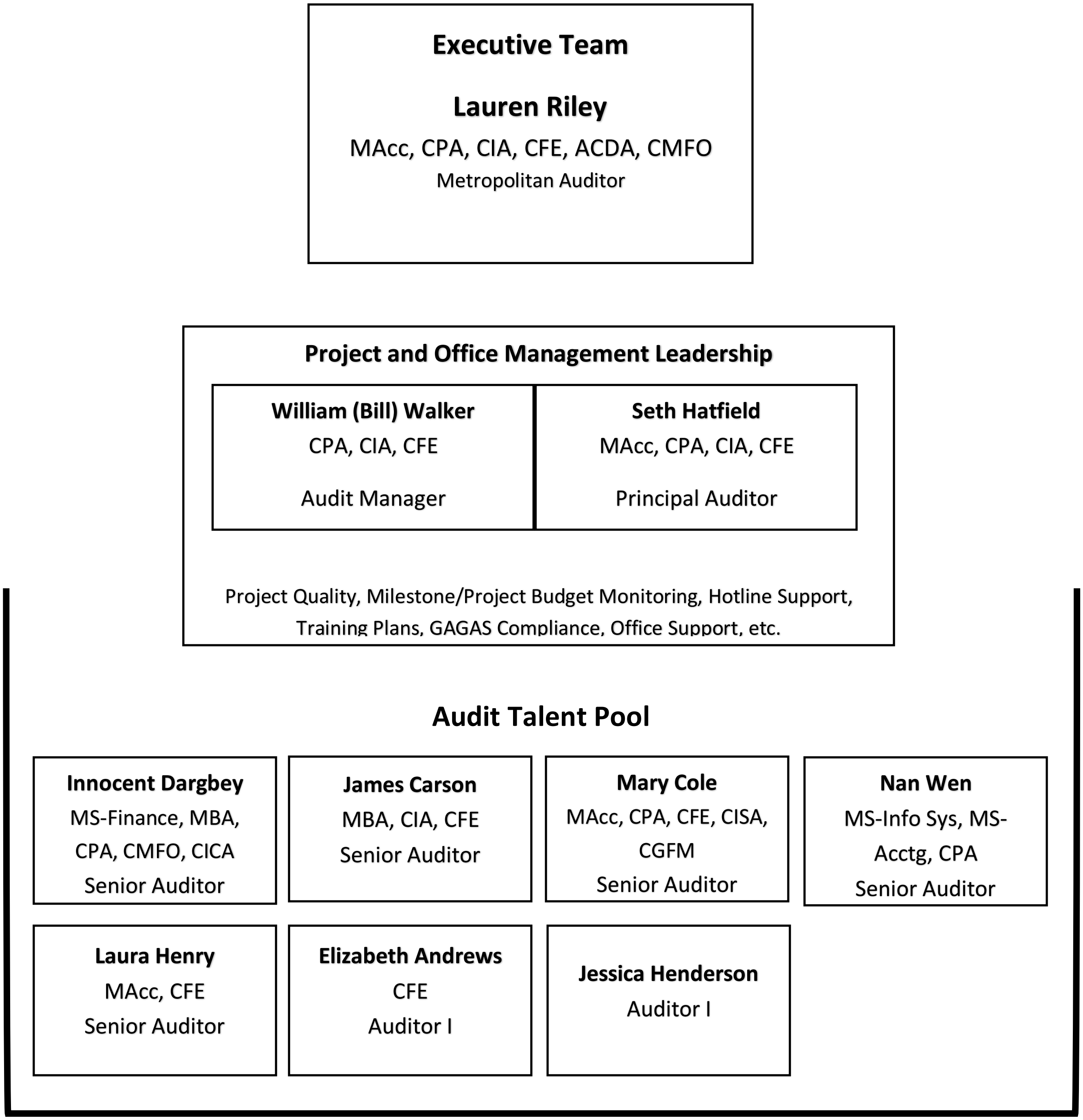
Office of Internal Audit Budget versus Actual
GSD General Fund as of March 31, 2022
FY 2022 Approved Budget

		FY 2022 Budget	Actual	Difference	Notes
Total Salaries & Fringe		$ 1,252,600	$ 770,677	$ 481,923	
Other Expenses					
Professional & Purchased Services		$ 192,200	$ 23,138	169,062	
Building Rent Parkway Towers		$ 59,500	$ 47,661	11,839	
Other Expenses		$ 77,600	$ 19,741	57,859	
Internal Service Fees		$ 51,300	$ 42,750	8,550	Information Technology
TOTAL EXPENSES		$ 1,633,200	$ 903,967	$ 729,233	**55% of budget used to date**

Office of Internal Audit Budget History

For the year ending June 30,	Co-sourcing Audit Budget	Total Budget	Co-sourcing Percent of Budget	FTE
2012	165,000	1,265,400	13%	10
2013	156,200	1,277,900	12%	10
2014	60,200	1,179,300	5%	10
2015	45,100	1,214,900	4%	10
2016	75,100	1,290,400	6%	10
2017	125,100	1,382,900	9%	10
2018	248,000	1,545,700	16%	10
2019	248,000	1,566,100	16%	10
2020	248,000	1,574,900	16%	10
2021	195,800	1,565,100	13%	10
2022	192,200	1,633,200	12%	10

Metropolitan Nashville Office of Internal Audit



Executive Team

Lauren Riley
MAcc, CPA, CIA, CFE, ACDA, CMFO
Metropolitan Auditor

Project and Office Management Leadership

William (Bill) Walker
CPA, CIA, CFE
Audit Manager

Seth Hatfield
MAcc, CPA, CIA, CFE
Principal Auditor

Project Quality, Milestone/Project Budget Monitoring, Hotline Support, Training Plans, GAGAS Compliance, Office Support, etc.

Audit Talent Pool

Innocent Dargbey
MS-Finance, MBA, CPA, CMFO, CICA
Senior Auditor

James Carson
MBA, CIA, CFE
Senior Auditor

Mary Cole
MAcc, CPA, CFE, CISA, CGFM
Senior Auditor

Nan Wen
MS-Info Sys, MS-Acctg, CPA
Senior Auditor

Laura Henry
MAcc, CFE
Senior Auditor

Elizabeth Andrews
CFE
Auditor I

Jessica Henderson
Auditor I

METROPOLITAN NASHVILLE AUDIT COMMITTEE
2022 MEETING PLAN

Meeting Date	Proposed Agenda Topics
February 8, 2022 (Tuesday)	• Office of Internal Audit Annual Performance Report • Internal Audit Annual Work Plan approval • Internal Audit issued report discussion • Open Audit Recommendations Status
April 12, 2022 (Tuesday)	• Election of Chairman and Vice Chairman • External Audit Single Audit and Management Letter presentation • Metropolitan Auditor performance review • Internal Audit issued report discussion • Open Audit Recommendations Status
June 14, 2022 (Tuesday)	• FY2022 External Audit plan and required communications • Internal Audit issued report discussion • Open Audit Recommendations Status
September 13, 2022 (Tuesday)	• Metropolitan Audit Committee self-assessment • Bylaws annual review • Internal Audit issued report discussion • Open Audit Recommendations Status • External Audit Comprehensive Annual Financial Report Audit Progress Executive Session
November 8, 2022 (Tuesday)	• Internal Audit issued report discussion • Open Audit Recommendations Status • External Audit Comprehensive Annual Financial Report Audit Progress Executive Session
December 13, 2022 (Tuesday)	• External Audit Comprehensive Annual Financial Report • Open Audit Recommendations Status • Internal Audit issued report discussion

Metropolitan Nashville Audit Committee

Executive Session Checklist

☑ The published agenda must disclose the general nature of the items to be discussed in executive session.
See, T.C.A. §9-3-405(f)

☑ All business which is public in nature shall be conducted first.
See, T.C.A. §9-3-405(g)(1)

☑ During the regular public session committee must vote to go into private executive session. Must obtain a majority to be successful.
See, T.C.A. §9-3-405(d)

☑ Chair must announce during the public portion of the meeting that no business other than the matters stated generally on the published agenda shall be considered during the confidential executive session.
See, T.C.A. §9-3-405(e)

☑ Adjourn the public portion of the meeting.
See, T.C.A. §9-3-405(g)(2)

☑ Only individuals whose presence is reasonably necessary in order for the committee to carry out its executive session responsibilities may attend the portion of the executive session relevant to that person's presence.
See, T.C.A. §9-3-405(h)

Permissible Executive Session Subject Matter

1. Items deemed not subject to public inspection under §§ 10-7-503 and 10-7-54, and all other matters designated as confidential or privileged under this code
2. Current or pending litigation and pending legal controversies
3. Pending or ongoing audits or audit related investigations
4. Information protected by federal law
5. Matters involving information under § 9-3-406 where the informant has requested anonymity
   See, T.C.A. § 9-3-405(d)