FINAL REPORT

A Report to the Audit Committee

Mayor
Freddie O'Connell

Director of Justice Integration Services
Nathalie Stiers

Audit Committee Members
Burkley Allen
Tom Bates
Angie Henderson
Courtney Johnston
Jenneen Reed
Matthew Scanlan

Justice Integration Services (JIS) 2024 Information Technology Audit

January 13, 2025

Due to the sensitive information included in this report, which could detail vulnerabilities, weaknesses, and possible threats to the operation of Justice Integration Services (JIS), the distribution for the full confidential report is limited to management of Justice Integration Services, Information Technology Services, and others in the local government with security clearance. This exemption is granted by Tennessee Code Annotated §10-7-504(i)(1) "Information that would allow a person to obtain unauthorized access to confidential information or to government property shall be maintained and confidential."

Metropolitan Nashville Office of Internal Audit

JUSTICE INTEGRATION SERVICES (JIS) 2024 INFORMATION TECHNOLOGY AUDIT

EXECUTIVE SUMMARY
January 13, 2025

Why We Did This Audit

The audit was performed due to the importance of ensuring information technology services are provided effectively to justice agencies.

What We Recommend

- Management should enforce separation of duties.
- [redacted]
- [redacted]
- Develop & document strategies for BC/DR plan validation.
- Update the password parameters to be compliant with the established policy, where possible.
- Formalize and optimize the change management process.

BACKGROUND

The mission of the Justice Integration Services department is to provide customized, integrated case management software and technology support products to Metropolitan Nashville justice agencies so they can manage and use shared information to improve the administration of justice for the Nashville community.

OBJECTIVES AND SCOPE

Frazier & Deeter, LLC. was engaged by the Office of Internal Audit to conduct an Information Technology audit of the Justice Integration Services department. The engagement aimed to evaluate the effectiveness of general information technology and application controls within the department. Additionally, Frazier & Deeter evaluated opportunities to improve the efficiency and effectiveness of the department's internal control environment.

The scope of the audit evaluated control objectives from August 1, 2023, through July 31, 2024.

WHAT WE FOUND

During fieldwork, we identified control deficiencies and areas of improvement which require attention from JIS management, which are communicated in the form of "findings". The table below indicates the total number of findings by control domain.

Control Domain	Results
Logical Access	One (1) finding noted.
Change Management	Two (2) findings noted.
Application Security	One (1) finding noted.
Information Security	One (1) finding noted.
Computer Operations	No findings noted.
Business Continuity	One (1) finding noted.
Endpoint Protection	No findings noted.

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:

- Frazier & Deeter, LLC. was hired to assist with this engagement.
- The detailed methodology employed by Frazier & Deeter, LLC. can be found in **Appendix A.**

AUDIT TEAM

Frazier & Deeter, LLC., Consultant

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

APPENDIX A – REPORT FROM FRAZIER & DEETER, LLC.

Frazier & Deeter, LLC. was hired to assist with this engagement. The firm issued a report to the Office of Internal Audit, with details on objectives, methodology, findings, and recommendations. The report begins on the next page.

2024

Justice Integration Services (JIS) 2024 Information Technology Audit

Metropolitan Government of Nashville & Davidson County

FRAZIER & DEETER

Table of Contents

Executive Summary

Background & Objectives

Frazier & Deeter ("FD") was engaged by the Metropolitan Government of Nashville & Davidson County Office of Internal Audit ("Metro" or "the Organization") to conduct an Information Technology ("IT") audit of the Justice Integration Services ("JIS") department. This engagement aimed to evaluate the effectiveness of general IT and application controls within the JIS department. Additionally, we evaluated opportunities to improve the efficiency and effectiveness of the JIS internal control environment.

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 observations and conclusions based on our audit objectives.

Our procedures did not constitute an engagement to provide financial audit, compilation, review, or attestation services as described in the pronouncements on professional standards established by the American Institute of Certified Public Accountants ("AICPA"), or other regulatory body and, therefore, we do not express an opinion or any other form of assurance.

Scope

The scope of the audit was determined based on identified risks and control objectives relevant to the JIS department's operations. For the period August 1, 2023, through July 31, 2024, the following control domains were evaluated:

- Logical Access
- Change Management
- Application Security
- Information Security
- Computer Operations
- Business Continuity
- Endpoint Protection

JIS and Metro have joint responsibility for certain aspects of the IT control environment. However, our procedures were limited to IT controls and processes that are performed by JIS and does not include controls and processes that fall under the management of the Metro Information Technology Services (ITS) department.

A summary of our control testing methodology and details on specific procedures performed are outlined in Appendix A.

Conclusion & Overall Rating

Results Summary by Control Domain

During fieldwork, we identified control deficiencies and areas of improvement which require attention from JIS management, which are communicated in the form of "findings". The table below indicates the total number of findings by control domain.

Control Domain	Results
Logical Access	One (1) finding noted.
Change Management	Two (2) findings noted.
Application Security	One (1) finding noted.
Information Security	One (1) finding noted.
Computer Operations	No findings noted.
Business Continuity	One (1) finding noted.
Endpoint Protection	No findings noted.

Finding Summary with Risk Ratings

The risk ratings for findings were assessed based on the likelihood and impact of a related adverse event that could prevent JIS and the Metropolitan Government of Nashville & Davidson County from meeting operational, financial, legal, and regulatory objectives and requirements. Risk ratings for findings identified are summarized in the table below.

Finding	Domain	Description	Risk Rating
F.1	Change Management	Segregation of Duties	High
F.2	Application Security	[redacted]	Medium
F.3	Information Security	[redacted]	Medium
F.4	Business Continuity	Business Continuity Planning	Low
F.5	Logical Access	Password Management	Medium
F.6	Change Management	Change Authorization & Documentation	Low

Details related to the deficiencies summarized in the table above, along with recommendations for improvement and management's action plans are detailed in Appendix B.

Overall Rating

Based on the results of our procedures, findings identified, and the aggregation of risk ratings assigned to these findings, we have assessed an overall rating of **Satisfactory** for the JIS department. Overall audit rating and deficiency risk rating definitions are detailed in Appendix C.

****

We would like to extend our sincere gratitude to the management of the JIS department and the Metropolitan Government of Nashville & Davidson County Office of Internal Audit for their cooperation and assistance throughout this audit. If you have any questions, please contact Brandon Sherman, Partner with Frazier & Deeter, LLC.

Appendix A: Audit Methodology

Approach

The audit followed a phased approach, each phase with specific objectives and procedures. Planning procedures consisted of the following:

- Conducting walkthroughs with JIS' management and operations teams to identify key systems and processes supporting the overall objectives of JIS;
- Performing a risk assessment to identify and evaluate risks posed to JIS' information systems, personnel, and operations;
- Identifying and establishing relevant control objectives based on the results of the risk assessment; and
- Developing audit procedures to evaluate the effectiveness of control activities to meet the established control objectives.

Evaluation of the implementation, design, and operating effectiveness of relevant controls was performed using the following methods:

- Inspection of relevant JIS and Metropolitan Government of Nashville & Davidson County policy and process documentation;
- Inquiries of JIS management to determine whether established policies and procedures have been implemented and are consistently applied;
- Inspection and observation of key application and system settings; and
- Sample-based testing of specific control activities performed by JIS to evaluate the operating effectiveness of such controls.

Detailed Testing Procedures

The procedures outlined below were designed to assess the control objectives within each of the identified domains. As such, the following audit steps were taken:

- **Logical Access**: Evaluated user access management processes, including the provisioning, modification, and termination of user access. Evaluated password management policies and practices. Examined access controls for source code repositories & deployment tools.

- **Change Management**: Assessed the processes for authorizing, testing, documenting, and deploying changes to IT systems and applications. Evaluated controls in place to enforce segregation of duties when making changes to in-scope systems.
- **Application Security**: Evaluated the frequency and effectiveness of application security processes, such as penetration tests and vulnerability scans.
- **Information Security**: Assessed audit logging and monitoring procedures to ensure timely detection and response to security incidents.
- **Computer Operations**: Assessed server management practices, including monitoring and maintenance procedures.
- **Business Continuity**: Evaluated the adequacy and effectiveness of disaster recovery and business continuity plans, including backup and restoration processes.
- **Endpoint Protection**: Assessed workstation management practices, focusing on encryption and antivirus measures.

Appendix B: Findings & Recommendations

F.1 – Segregation of Duties

Finding:
FD identified seven (7) users who have both the ability to develop and promote code to production. These users are part of the software development team and possess access to source code repository management tools, as well as access to migrate changes to production.

Risk:
Developers having access to both development and production environments for JIS applications can increase the risk that unauthorized or inadvertent changes in the production environment may occur, compromising the security and integrity of the applications.

Recommendation:
Management should enforce separation of duties by restricting access so that the developer of a change cannot also migrate the change to production. However, if the current user-role assignments are necessary to sustain operations, management could conduct monthly audits of changes migrated to the production environment to verify the changes followed the established change management processes (e.g. security risk assessments, approval by end-user, etc.).

Management Action Plan:
Due to the limited number of development staff, it is not possible to enforce a segregation of duties within JIS. Therefore, JIS management will implement a process to review and audit all changes pushed into the production environment.

Management Implementation Date:
03/31/2025

F.2 – [redacted]

F.3 – [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

F.4 – Business Continuity Planning

Finding:
The current JIS Business Continuity and Disaster Recovery plan ('JIS Disaster Recovery Plan') requires quarterly testing and maintenance; however, management has not implemented a formal process for business continuity and disaster recovery plan testing, maintenance, or review by appropriate personnel.

Risk:
Insufficient plan testing & review could result in an inadequate response to a disaster or business interruption, potentially leading to prolonged system downtime and operational disruption for JIS.

Recommendation:
Develop & document strategies for BC/DR plan validation, including testing procedures, review cadence, and necessary stakeholders. Define owners responsible for reviewing, testing & approving revisions of the plan, at least annually. In addition, JIS should develop a plan for periodically testing the BC/DR plan.

Note: Management noted there is an organizational effort being conducted by Metro leadership, in which they assist the departments with developing and/or updating their disaster recovery & business continuity plans. Given this initiative, the tenure of JIS staff deemed to be key in the recovery process, and clear designation of roles & responsibilities if a disaster were to be declared, noted management is taking action to reasonably mitigate the risk(s) posed to JIS and its customers by lack of annual BC/DR plan testing & review. However, management should take steps necessary to ensure the established policy is aligned with JIS-specific procedures.

Management Action Plan:
JIS has been selected to participate in phase 2 of the overall Metro Business Continuity and Disaster Recovery review process. JIS management will work with the Metro BC/DR committee to update the current JIS BC/DR document and JIS management will review that document annually to ensure that the information within remains up to date.

Management Implementation Date:
06/30/2025

F.5 – Password Management

Finding:
Although there are user access control mechanisms at JIS, including Multi-Factor Authentication (MFA) enabled for the JIS Nashville domain and subsequent mandatory AD authentication for application & database access, certain password parameters for JIS' applications and databases are not configured according to Metropolitan Government of Nashville and Davidson County Information Security standards.

Risk:
Inadequate password management could lead to identity theft and unauthorized access, compromising individual applications and potentially leading to a broader security breach.

Recommendation:
JIS should update the password parameters to be compliant with the established policy, where possible. For passwords that cannot meet the Information Security standards, a formal exception process should be established to acknowledge noncompliant configurations and document any applicable mitigating factors.

Management Action Plan:
As the applications exist today, Oracle does not natively offer the ability to configure all complexity settings necessary to comply with the Metro password requirements. JIS will be replacing selected older applications with new vendor-supported solutions. Any vendor-purchased solution will be required to comply with the Metro password complexity requirements. JIS will be modernizing the applications that will not be replaced with vendor-purchased solutions. As such, JIS will ensure that these applications comply with the Metro password complexity requirements. Any noncompliant applications following this process will be documented.

Management Implementation Date:
This is an ongoing process and implementation dates will vary based on the application.

F.6 – Change Authorization & Documentation

Finding:
The process for ensuring consistent evidence of testing and approval of changes to JIS applications is not formally documented. Although test scripts, testing evidence, and approvals for changes are available via emails and/or shared drives, the lack of a formalized documentation retention process could result in loss of supporting documentation for system changes.

Risk:
The absence of a formalized process for documenting testing and approval increases the risk that changes may be implemented without proper verification, potentially leading to system errors and operational disruptions.

Recommendation:
Management should formalize and optimize the change management process. This includes defining where information related to changes should be stored, specifying the status that changes must be marked as when complete, and detailing the type of evidence that must be saved. Implementing a standardized procedure within Jira for documenting evidence of testing performed by the developer, as well as end-user testing and approval, will ensure changes are properly verified before being promoted to production.

Management Action Plan:
JIS currently has a documented change management process with corresponding documentation, which includes signoffs and testing documentation. However, this documentation is stored in multiple locations. Management will ensure that all relevant testing documentation and approvals are attached to the JIRA ticket for each application change.

Management Implementation Date:
03/31/2025

Appendix C: Audit & Risk Rating Definitions

Ratings – Overall Audit – General Guidelines

Overall Audit ratings are based on the condition of the overall audit results and issues at the time of the audit, not at the time of the issuance of the report. The Overall Audit rating may not be affected by addressing the issues prior to the distribution of this report. Overall Audit ratings shall be based on, but not limited to, the following criteria:

Overall Audit Rating	Definition
Outstanding	Effective controls exist, except for a few minor findings.
Satisfactory	Acceptable controls are in place, except for some findings which require remediation from management. The system of internal control, as designed, provides general assurance that significant objectives will be achieved.
Needs Improvement	Deficiencies in controls exist which due to the frequency or severity, require increased management attention and improvement.
Unsatisfactory	Controls require immediate improvement and management action. The system of internal control, as designed, does not provide assurance that significant objectives will be achieved.

Individual finding risk ratings are based upon the likelihood and impact of a risk occurring due to the failure of the noted control at the time of the audit. Individual finding risk ratings are based on, but not limited to, the following criteria:

Finding Risk Rating	Definition
Critical	The threat imposed by the risk is extremely likely to occur and likely would result in the material loss of assets, significantly impede or prevent normal operations, and/or likely would cause death or serious injury. An immediate, comprehensive corrective action plan should be implemented immediately by management upon identification with progress monitored by an appropriate level of management.
High	A risk that may have a significant impact on the organization's performance, reputation/brand, or cause disruption to normal business operations. Identified deficiencies warrant immediate attention by management.
Medium	Risks that could have a moderate impact on the organization's financials, operational effectiveness, or regulatory compliance. Identified deficiencies should be corrected promptly by management to ensure the internal control systems are functioning adequately.
Low	A risk that may have a minor effect or consequence on the organization's financials, operations, or regulatory compliance. Typical findings are isolated, management is aware of expected controls, and remediation is easily achieved by the reiteration of proper procedures or coaching of employees.

APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN

JIS justice integration services

January 3, 2025

Ms. Lauren Riley,

This letter acknowledges that Justice Integration Services (JIS) has reviewed the findings of the technical audit performed by Frazier and Deeter. JIS will work to implement the recommended improvements as outlined in the responses to each item.

It was a pleasure working with the team at Frazier and Deeter.

Sincerely,

Nathalie Stiers, DSL, Department Head
Justice Integration Services

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.

Risk	Recommendations	Concurrence and Action Plan	Proposed Completion Date
H	**F.1 -** Management should enforce separation of duties by restricting access so that the developer of a change cannot also migrate the change to production. However, if the current user-role assignments are necessary to sustain operations, management could conduct monthly audits of changes migrated to the production environment to verify the changes followed the established change management processes (e.g. security risk assessments, approval by end-user, etc.).	Due to the limited number of development staff, it is not possible to enforce a segregation of duties within JIS. Therefore, JIS management will implement a process to review and audit all changes pushed into the production environment.	3/31/2025
M	**F.2 -** [redacted]	[redacted]	This is an ongoing process and implementation dates will vary based on the application.
M	**F.3 -** [redacted]	[redacted]	3/31/2025

APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN

Risk	Recommendations	Concurrence and Action Plan	Proposed Completion Date
L	**F.4 -** Develop & document strategies for BC/DR plan validation, including testing procedures, review cadence, and necessary stakeholders. Define owners responsible for reviewing, testing & approving revisions of the plan, at least annually. In addition, JIS should develop a plan for periodically testing the BC/DR plan.	JIS has been selected to participate in phase 2 of the overall Metro Business Continuity and Disaster Recovery review process. JIS management will work with the Metro BC/DR committee to update the current JIS BC/DR document and JIS management will review that document annually to ensure that the information within remains up to date.	6/30/2025
M	**F.5 -** JIS should update the password parameters to be compliant with the established policy, where possible. For passwords that cannot meet the Information Security standards, a formal exception process should be established to acknowledge noncompliant configurations and document any applicable mitigating factors.	As the applications exist today, Oracle does not natively offer the ability to configure all complexity settings necessary to comply with the Metro password requirements. JIS will be replacing selected older applications with new vendor-supported solutions. Any vendor-purchased solution will be required to comply with the Metro password complexity requirements. JIS will be modernizing the applications that will not be replaced with vendor-purchased solutions. As such, JIS will ensure that these applications comply with the Metro password complexity requirements. Any noncompliant applications following this process will be documented.	This is an ongoing process and implementation dates will vary based on the application.
L	**F.6** Management should formalize and optimize the change management process. This includes defining where information related to changes should be stored, specifying the status that changes must be marked as when complete, and detailing the type of evidence that must be saved. Implementing a standardized procedure within Jira for documenting evidence of testing	JIS currently has a documented change management process with corresponding documentation, which includes signoffs and testing documentation. However, this documentation is stored in multiple locations. Management will ensure that all relevant testing documentation and approvals are attached to the JIRA ticket for each application change.	3/31/2025

APPENDIX B – MANAGEMENT ACCEPTANCE AND CORRECTIVE ACTION PLAN

Risk	Recommendations	Concurrence and Action Plan	Proposed Completion Date
	performed by the developer, as well as end-user testing and approval, will ensure changes are properly verified before being promoted to production.		