Montgomery County, Maryland
Office of the County Executive
Office of Internal Audit

Data Security and Governance Audit

September 30, 2024

Highlights

Why MCIA Did this Review

The Montgomery County Office of Internal Audit (MCIA) conducted a Data Security and Governance audit across selected departments of Montgomery County (the County). The County's IT functions are both centralized and de-centralized. Therefore, each department reviewed has unique Data Security and Governance responsibilities with varying amounts of assistance from Technology and Enterprise Business Solutions (TEBS). The audit assessed data governance policies, procedures, training, awareness, privacy impact assessment, business management of data, data use and retention, electronic and physical record management, transfer of data, data at rest, third-party interaction with data, and applicable incident response considerations.

Additionally, the audit reviewed inventory management of all sensitive records, data systems maintenance, data classification, management of data content, data handling, and levels of data access defined and assigned to individuals based on their roles and responsibilities in the County.

The audit was conducted by the accounting firm SC&H Group, Inc., under contract with MCIA.

September 2024

Data Security and Governance Audit

What MCIA Found

The audit of Data Security and Governance determined that established processes and controls reduce the risk of unauthorized access, usage, data modification, data transfer, data disclosure, data theft, loss of data and corruption.

The audit identified five areas of improvement to strengthen controls and mitigate risks within the County's IT Data Security and Governance processes.

1. Data classification policy and procedure management.
2. Security awareness training.
3. Data privacy policy and procedure management.
4. Third-party contract management respective to expectations for management and treatment of PII.
5. Third-party system periodic review.

TABLE OF CONTENTS

Objectives

This report summarizes the results of an audit of Montgomery County Government's (County) Data Security and Governance program as designed and implemented within selected departments based on data asset criticality (audit). The audit was performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County Office of Internal Audit (MCIA).

The audit's objectives were to:

1. Determine if appropriate levels of authority are assigned and proactively define the scope and limitations of that authority as a prerequisite to successful data management.
2. Determine if organizational structure with appropriate levels of data governance has been established, and roles and responsibilities at various levels specified (e.g., governance committee members, technology leaders, data stewards, etc.).
3. Ensure clear policies and procedures are in place to communicate and ensure the importance of data quality and security throughout the organization.
4. Ensure an up-to-date inventory of all sensitive records and data systems is maintained, including those used to store and process data, that enables the organization to target its data security and management efforts.
5. Determine data classification and management of data content, including identifying the purposes for which data are collected, are defined to justify the collection of sensitive data, optimize data management processes, and ensure compliance with federal, state, and local regulations.
6. Ensure appropriate data handling is in place to provide data stewards and users with appropriate tools for complying with an organization's security policies.
7. Determine if established and regularly updated strategies for preventing, detecting, and correcting errors in and misuses of data are in place.
8. Ensure differentiated levels of data access are defined and assigned to individuals based on their roles and responsibilities in the organization to prevent unauthorized access and minimizing the risk of data breaches.

Background

County-wide Information Technology Overview

The County manages hardware, software, and technology through a combination of centralized and decentralized functions to enable employees to deliver quality services to citizens and businesses, provide information and services efficiently, and enhance productivity.

Technology and Enterprise Business Solutions (TEBS) is responsible for assisting the County's departments with identifying innovative technology solutions, helpdesk support, IT security, IT asset procurement and management, data security, data management and governance, and access management for Active Directory (AD) and Oracle Enterprise Resource Planning (ERP).

Data Security and Governance

Data governance is a set of processes that ensures data assets are formally managed throughout the enterprise. A data governance model establishes authority, management, and decision-making parameters related to the data produced or managed by the enterprise. Data Security and Governance is managed through having an established set of standards, policies, procedures, and controls in place. The policies set expectations regarding how data is stored, gathered, processed, and disposed of. By having effective and detailed policies and procedures, organizations can achieve confidentiality, integrity, and availability of data assets. As defined by

National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 IT governance framework, the following domains are considered key areas within Data Security and Governance:

Governance Policy and Procedures: The organization has established, communicated, and monitors its Data Security and Governance strategy, expectations, and policy.

Training and Awareness: The organization provides its personnel with data security and cybersecurity awareness training to enable them to perform their cybersecurity-related tasks.

Privacy Impact Assessment: The organization has defined criteria for Privacy Impact Assessments (PIA) that are included in business processes and changes within the organization.

Business Management of Data: The organization has established policies and procedures to distinguish between unique identifiers treated as personally identifiable information (PII), aggregate information, and de-identified information.

Use and Retention: The organization/system owner obtains consent when collecting data for applicable information systems.

Electronic and Physical Records Management: The organization has established records management policies and procedures for the retention, storage, and disposal of data throughout the organization.

Transfer of Data: The organization has data loss prevention tools in place to monitor and enforce data transfers.

Data at Rest: The organization has data encryption standards in place for data at rest, which are enforced throughout the enterprise.

Third-party Interaction with Data: The organization manages third parties through contracts that detail the management and treatment of PII. Furthermore, the organization has established a process to assess third-party service providers, which is managed and reviewed by the enterprise.

Incident Response and Escalation Plan: The organization has established an incident response plan that is reviewed and updated on an annual basis and includes appropriate breach escalation procedures.

External Party Notifications: The organization contractually requires third-party service providers and vendors managing PII to notify the enterprise in the event of breaches.

Scope and Methodology

The audit was performed in accordance with the Statement on Standards for Consulting Services (SSCS) issued by the American Institute of Certified Public Accountants (AICPA). In addition, NIST Special Publications SP 800-53 IT governance framework was used to supplement the performance of the audit over Data Security and Governance. The audit was conducted from October 2023 to April 2024.

The audit focused on the overall strategic approach to implementation and effectiveness of Data Security and Governance processes and subprocesses in selected departments throughout the County.

The audit scope included review of the following:

1. Data management policies, procedures, content, and document development to ensure data management functions are performed in a standardized manner for County employees, vendors, and contractors.
2. Data management processes and supporting activities from other processes necessary to manage:
    a. Data access authority and scope limitations.
    b. Data classification and management of data content.
    c. Data collection and define justification for collection of sensitive data.
    d. Data handling requirements.
3. Inventory of defined sensitive records and data systems that store and process data.
4. Data management regulations from the federal, state, and local jurisdictions.
5. Data error and misuse prevention, detection, and correction strategies.

Process Understanding

SC&H performed the following procedures to understand the processes, risks, and controls related to the scope of the audit. SC&H obtained and reviewed both department level and TEBS data governance policies and procedures. Further, SC&H conducted meetings with selected departments that focused on assessing the existing process and procedures that are in place for Data Security and Governance at the department level.

Phase 1 Planning

SC&H initially performed a planning phase designed to determine the scope of departments to be included within Phase 2 Fieldwork. SC&H leveraged information gathered by the County's Business Impact Analysis (BIA) project, conducted by SC&H, as a resource for identifying and assessing departments and/or divisions to be considered for testing. SC&H selected and agreed upon eight departments and/or divisions (collectively "departments") to be included within scope of Phase 2 Fieldwork.

Phase 2 Fieldwork

Based on the understanding of the processes, risks, and associated controls established during the process understanding procedures, SC&H developed an audit program designed to meet the audit's objectives, which included procedures to validate the design and effectiveness of departmental Data Governance and Security controls.

In order to achieve the objective of evaluating the data governance and security at Montgomery County effectively, SC&H primarily relied on the security control framework provided by NIST SP 800-53 Rev.5[1]. NIST is a widely recognized framework globally, designed to provide guidance to industry, government agencies, and other organizations to manage cybersecurity risks. Cybersecurity risks are expanding constantly, and managing those risks must be a continuous process.

[1] "Security and Privacy Controls for Information Systems and Organizations." *NIST SP 800-53 Rev. 5*, 10 Dec. 2020, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Additionally, SC&H incorporated supplementary controls to address specific objectives and concerns that were identified during departmental interviews and review of Enterprise policies and procedures. This approach ensured a comprehensive evaluation of the County's data governance and security practices.

SC&H executed fieldwork testing by following the fieldwork audit work program for eight selected departments. SC&H achieved each audit objective by conducting specific tasks that included inquiries, observations, and the inspection of documentation provided by the departments. Additionally, SC&H selected samples of application systems within select departments responsible for storing and processing sensitive data to verify compliance with agency and division-level data governance policies and procedures in accordance with audit objectives.

Interviews

SC&H conducted detailed interviews and walkthroughs with the selected departments. The purpose was to observe and document the internal controls and related risks associated with each of the following domains:

1. Governance Policy and Procedures
2. Training and Awareness
3. Privacy Impact Assessment
4. Business Management of Data
5. Use and Retention
6. Electronic and Physical Records Management
7. Transfer of Data
8. Data at Rest
9. Third-party Interaction with Data
10. Incident Response and Escalation Plan
11. External Party Notifications

Policy and Procedure Review

SC&H obtained and reviewed data security governance policies and procedures from the selected departments and TEBS.

SC&H obtained the following documents:

1. Administrative Procedure 6-7, Information Security including the Information Security System and Data Owners Handbook and the Information Security Rules of Behavior Handbook, which is the County’s established policies and procedures for compliance with information security policy in the use of the County’s technological devices. AP 6-7 includes, but is not limited to the following areas related to Data Security and Governance:
    a. Information System Access Control
    b. Information Security Awareness and Training
    c. Information Security Assessments and Privacy Assessments, Authorization, and Monitoring
    d. Identification and Authentication
    e. Incident Response
    f. Risk Assessment
    g. Personnel Security
2. Administrative Procedure 6-3, Records Management, which establishes a framework to manage maintenance, distribution, storage, preservation, and disposal of all records for all County departments.

3. Administrative Procedure 6-1, Use of County-Provided Technology, which provides a framework for the following:
    a. General Connecting to Internet, Intranet, and email Services
    b. Prohibited User Conduct
    c. County Ownership, Monitoring, Control and Disclosure

Test Plan Development
Utilizing the information obtained during the scoping and departmental interviews and walkthrough procedures, SC&H developed an audit program to test the design and/or operational effectiveness of internal controls identified.

Testing
Fieldwork consisted of testing the design and operational effectiveness of internal controls identified during the scoping and preliminary departmental assessment, interviews, and walkthrough procedures. SC&H prepared a document request listing for all information needed to satisfy the testing steps developed in the audit plan, including populations required to select samples for which additional information was requested. SC&H utilized both judgmental and random selection methods for sampling.

SC&H selected a representative sample of information systems that store, process, or transmit sensitive data for each in-scope department. The samples included both internally and third-party managed systems. SC&H haphazardly selected a minimum of one and no more than three samples for each in-scope County department function.

Validation
The preliminary test results were compiled and presented to the selected departments. Appendix A is provided as reference for all controls tested as part of the audit.

Findings and Recommendations

The following six finding categories and associated recommendations are a compilation of observations identified during the audit. These recommendations were designed to strengthen and expand departmental Data Security and Governance processes and controls.

Due to the sensitive nature of the specific department findings, certain detailed information is not included in this report. Department-specific findings and recommendations have been communicated directly with each department; each department will be required to develop corrective action plans to timely and fully address the recommendations. Summary-level findings are discussed below, without attribution to specific departments. Certain findings, identified below, require enterprise-level action by TEBS. TEBS will be responsible for developing a corrective action plan to address these applicable findings and recommendations.

Finding 1: Data Classification Policies and Procedures
Background The purpose of data classification is to organize data into distinct categories so it can be used, protected, stored, and accessed accordingly. Data can be classified into various categories such as confidential, critical, sensitive, public, internal, PII and protected health information (PHI). Data classification policies and procedures provide specific directions and set certain expectations to manage defined data sets. Based on the policies and procedures, data should be classified, and appropriate data security standards should be applied to manage risk effectively.

Finding 1: Data Classification Policies and Procedures

Finding
The County does not currently have a clear formal data classification policy that identifies specific categories of data, with the associated policy and procedure requirements applicable to each category. Based on inquiry performed we noted that TEBS, in coordination with the Office of the County Attorney and departments is in the process of developing an enterprise-wide data classification policy. An interim Administrative Procedure 6-12, Data Classification, has been developed and issued; this interim AP was issued subsequent to the audit period.

Risks
Lack of a sufficient data classification policy could lead to a lack of direction or unclear expectations regarding treatment of sensitive data. This could further lead to all data being treated the same across the organization and lack of sufficient security controls around critical and sensitive data.

Recommendation 1
TEBS should continue development of County data classification policies and procedures. Any changes to policies and procedures related to data classification, should be communicated to appropriate stakeholders throughout the organization.

Finding 2: Security Awareness Training

Background
Security awareness program training is conducted on a defined periodic basis which includes data governance and security topics such as password management, social media safety, email security, identify & theft, and data privacy. Attendance and completion of this required monthly training is tracked.

Finding
The details related to this finding have been communicated to the respective department(s).

Risks
Not completing security training for all employees could lead to a potential vulnerability which could ultimately lead to data breach or loss of sensitive information unintentionally by employees.

Recommendation 2
TEBS should work with departments to apply standardized enforceable sanctions, with the support of HR, which promote timely completion of required security awareness training. In addition to currently designed reminders and follow up communication, the County should consider additional escalation in communication channels and define considerations for further disciplinary action.

Finding 3: Data Security and Privacy Plans

Background
The intent of data privacy policies and procedures is to provide clarity across the organization/department and set expectations regarding data collection, usage, storage, sharing, and transferring. These policies and procedures are essential in helping to comply with privacy regulations and requirements, such as Health Insurance Portability and Accountability Act (HIPAA). Organizations or departments should have clearly documented

Finding 3: Data Security and Privacy Plans

data privacy policies and procedures, and plans for specific information systems that should be reviewed periodically.

Finding

There are opportunities for improved development of data security and privacy policy plans for information systems across a number of departments. For select departments, privacy policy documents are reviewed but not updated to reflect completion of the review process.

Risks

Lack of appropriate data privacy plans for information systems could lead to inappropriate usage, sharing, transferring, or disclosure of data potentially violating privacy laws leading to violations and fines.

Recommendation 3

Departments should ensure that data privacy plans for information systems are sufficiently designed and implemented in accordance with requirement 2.12.1 of the Information Security System and Data Owners Handbook. Any updates should be communicated across the organization. In addition, applicable policies should be reviewed periodically, and evidence of review should be formally documented and retained.

Finding 4: Treatment and Management of PII in Third-Party Contracts.

Background

All contracts with third parties who handle sensitive or critical data should be detailed to clearly outline the security expectations and restrictions related to the treatment of associated data. All contracts should include the management and treatment of PII.

Finding

Requirements for the treatment of sensitive date, including Personally Identifiable Information (PII), were not included within a sample of one third-party management contract.

Risks

By not including language referencing management and treatment of PII, contracted third parties may not understand or be informed of their role and responsibility towards management and treatment of PII which could potentially lead to exposure, usage, transferring or sharing of data with an unauthorized party.

Recommendation 4

The County should ensure that all third-party contracts handling sensitive data include a section, or reference to executed business associate agreement (BAA), that clearly covers expectations for management and, as applicable, treatment of PII by the third-party based on enterprise policies and procedures.

Finding 5: Periodic Assessment of Third-party Systems.

Background

The growing risk of supply chain attacks makes it critical to monitor the level of risk posed to the organization by supply chain vendors and by their products or services. A third-party risk assessment quantifies the risks associated with third-party vendors and suppliers that provide products or services to the organization and have access to sensitive data. This assessment is useful for analyzing both new and ongoing supplier relationships. A periodic third-party risk

Finding 5: Periodic Assessment of Third-party Systems.

assessment, part of a third-party risk management program, evaluates all security-related considerations when outsourcing a product or service to a third-party. It typically involves establishing risk criteria and performing onboarding and periodic screening for third-party partners and vendors.

Finding

Periodic risk assessments were not performed for a sample of third-party systems.

Risks

Not performing periodic assessments of third parties increases the risk that sensitive data is not appropriately handled and/or secured. Additional third-party related risks can include financial risk, strategic risk, reputational risk, operational risk, cybersecurity risk, regulatory risk, and compliance risk.

Recommendation 5

As TEBS continues to design and develop a formal third-party risk management program, they should work with system owners across departments to ensure that all third-party systems with access to sensitive data are assessed and reviewed by appropriate stakeholders at least annually. Appropriate action(s) should be taken as a result of the review, if required. Results should be documented and maintained.

TEBS should consider updating AP 6-7 to include additional language outlining requirements for minimum annual review procedures of any third-party system with access to sensitive/critical data.

Comments and MCIA Evaluation

We provided the Technology and Enterprise Business Solutions (TEBS) with a draft of this report for review and comment. TEBS responded, concurring with the five recommendations, and provided a summary of the actions taken or in process to address the recommendations and to continue to work with departments to ensure that there are appropriate controls and management processes in place to enhance data security and governance.

No changes were made to the report based on the TEBS response.

Appendix A – Data Security and Governance

Domain	Control #	Control Description
Governance Policy and Procedures	DG.1	The roles and responsibilities regarding the management of data governance for privacy, confidentiality, and compliance are defined and cover key areas of process and technology across the enterprise.
	DG.2	Data privacy policies have been documented, approved, and communicated to the organization. The policy is reviewed and an approved on a defined frequency.
Training and Awareness	DG.3	The training and security awareness program includes data privacy. Attendance is tracked and all employees re-certify at least annually.
Privacy Impact Assessment (Risk Management)	DG.4	Criteria for Privacy Impact Assessments (PIA) are defined and included in business processes and changes within the organization. Tools and monitoring are in place to ensure compliance with assessment findings.
	DG.5	Data classification policies have been documented, approved, and communicated to the organization. The policy is reviewed and approved on a defined frequency.
Business Management of Data	DG.6	There are policies and procedures in place to distinguish unique identifiers treated as personally identifiable information, aggregate information, and de-identified information.
	DG.7	Data de-identification is enforced through tools and other automated means across the enterprise.
Use and Retention	DG.8	The system owner receives consent for data collection. Retention, storage, and disposal of data is clearly defined and implemented throughout the organization. If data is retained, returned, or used after the end of a contract it is clearly identified.
Electronic and Physical Records Management	DG.9	There are policies and procedures in place for records management. Retention procedures are identified, storage sites are managed, and disposal is enforced per retention schedule.
Transfer of Data	DG.10	The organization has data loss prevention tools in place to monitor and enforce data transfers.
Data at Rest	DG.11	Data encryption standards are in place for data at rest and enforced throughout the enterprise.

Third-party Interaction with Data	DG.12	Third parties are managed through contracts that detail the management and treatment of PII.
	DG.13	Third parties undergo an assessment that is managed and reviewed by the enterprise.
Incident Response and Escalation Plan	DG.14	The incident response plan is reviewed and updated on an annual basis and includes appropriate breach escalations procedures.
External Party Notifications	DG.15	Third-party vendors managing PII are contractually required to notify enterprise in the event of breaches.
	DG.16	The enterprise and third-party vendors have cyber insurance to protect client data in the event of a data breach. If cyber insurance is not obtained, a valid business reason is obtained for the lack of insurance.

Appendix B – Department Comments

DEPARTMENT OF TECHNOLOGY AND ENTERPRISE BUSINESS SOLUTIONS

Marc Elrich
County Executive

Gail M. Roper
Chief Information Officer/Director

MEMORANDUM

September 20, 2024

TO: **Bill Broglie, Internal Audit Manager**
Office of the County Executive

FROM: **Gail Roper, Director** *Gail Roper*
Department of Technology and Enterprise Business Solutions (TEBS)

SUBJECT: Formal Comments on Draft Report: "Information Technology Governance Evaluation" – September 2024

Enclosed please find the Department of Technology and Enterprise Business Solutions formal response to the Information Technology Governance Evaluation draft final report issued by Internal Audit.

If you or the audit firm working with you have any questions, please contact James Rogers or myself.

cc: Keith Young, Chief Information Security Officer, TEBS
Alison Dollar, Chief Budget Officer, TEBS
James Rogers, Policy Analyst, TEBS

TEBS welcomes the opportunity to use the findings of this report to improve the governance of IT across County Government. TEBS takes the responsibility of supporting County IT functions seriously and is committed to managing information security and cybersecurity controls, strengthening innovation, and building business continuity with an enterprise, whole-County approach.

Responses to the following specific recommendations are included, below:

2024 Recommendation #1: [Data Classification Policies and Procedures] TEBS should continue development of County data classification policies and procedures. Any changes to policies and procedures related to data classification, should be communicated to appropriate stakeholders throughout the organization.

Response: TEBS is developing the Data Classification Policy AP 6-12. The draft was sent for comment, several comments were received, and these are being considered. TEBS recognizes the importance of this policy and how much it interconnects with other departments. TEBS plans to finalize the AP as soon as possible in FY25, targeting the 3rd quarter, given the dependencies.

2024 Recommendation #2: [Security Awareness Training] TEBS should work with departments to apply standardized enforceable sanctions, with the support of HR, which promote timely completion of required security awareness training. In addition to currently designed reminders and follow up communication, the County should consider additional escalation in communication channels and define considerations for further disciplinary action.

Response: TEBS included in the AP 6-7 Information Security Rules of Behavior that the County must provide and monitor security awareness training and that users must complete all County Mandatory Security Awareness Training prior to the close of business on the last day of the same month in which the training was initiated. TEBS will continue to monitor compliance with the mandatory security awareness training requirement and determine whether additional actions need to be taken to enhance compliance. TEBS considers that this item is complete.

2024 Recommendation #3: [Data Security and Privacy Plans] Departments should ensure that data privacy plans for information systems are sufficiently designed and implemented in accordance with requirement 2.12.1 of the Information Security System and Data Owners Handbook. Any updates should be communicated across the organization.
In addition, applicable policies should be reviewed periodically, and evidence of review should be formally documented and retained.

Response: TEBS will begin working with departments to ensure they are building data privacy plans in accordance with requirement 2.12.1 of the Information Security System and Data Owners Handbook and that departments review those plans on a periodic basis.

- TEBS's Deputy Privacy Official will begin working with departments to ensure they are building data privacy plans for HIPAA in accordance with requirement 2.12.1 of the Information Security System and Data Owners Handbook. TEBS will meet with representatives of selected departments during the first quarter of CY 2025 to discuss the requirements set forth in the Handbook and to determine whether additional guidance to departments is necessary.
- TEBS will establish with each department an anticipated schedule for each selected department to develop privacy plans (where they do not exist) for identified systems.
- TEBS will conduct a periodic review of selected departments' compliance with the requirements of section 2.12.1 of the Handbook.

2024 Recommendation #4: [Treatment and Management of PII in Third Party Contracts] The County should ensure that all third-party contracts handling sensitive data include a section, or reference to executed business associate agreement (BAA), that clearly covers expectations for management and, as applicable, treatment of PII by the third-party based on enterprise policies and procedures.

Response: TEBS's Deputy Privacy Official will begin working with departments to ensure they are building data privacy plans in accordance with requirement 2.12.1 of the Information Security System and Data Owners Handbook. They are working with the members of the covered components to compile a list all currently active BAAs for their departments and to assess if any additional BAAs are needed. The Workgroup will also review the County's template BAA to see what, if any, changes need to be made. This item is in progress, and a schedule for future action will be developed once the Workgroup has met and discussed the issue.

2024 Recommendation #5: [Periodic Assessment of Third-Party Systems] As TEBS continues to design and develop a formal third-party risk management program, they should work with system owners across departments to ensure that all third-party systems with access to sensitive data are assessed and reviewed by appropriate stakeholders at least annually. Appropriate action(s) should be taken as a result of the review, if required. Results should be documented and maintained.

TEBS should consider updating AP 6-7 to include additional language outlining requirements for minimum annual review procedures of any third-party system with access to sensitive/critical data.

Response: TEBS has hired a third-party risk engineer who is working with departmental IT and legal staff on third-party contract risk management. TEBS, in conjunction with the risk engineer,

will work with system owners across departments to ensure that all third-party systems with access to sensitive data are assessed and reviewed by appropriate stakeholders. Appropriate action(s) should be taken as a result of the review, if required. Results should be documented and maintained. The requirement to conduct this annual review will be reflected in revised policy guidance issued by TEBS to departments. The expected timeframe for these actions will be determined in the near future.

Additionally, the updated AP 6-7 ISSADoH section 1.2 includes language requiring third parties to be assessed and for third-party contracts to include adequate language and safeguards. This section is closed.

TEBS appreciates this opportunity to provide formal response.