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

Montgomery County Government
Information Technology Governance Evaluation

September 29, 2023

MCIA-23-3

Highlights

Why MCIA Did this Review

The Montgomery County Office of Internal Audit (MCIA) conducted an Information Technology (IT) evaluation of the County's IT governance program.

The County's IT functions are both centralized and de-centralized. Therefore, each department reviewed has unique IT governance responsibilities with varying amounts of assistance and oversight from the Department of Technology and Enterprise Business Solutions (TEBS). This evaluation assessed the policies and procedures surrounding the IT governance program, its alignment with organizational objectives, the identification and management of risks, the optimization of IT investments, the identification of IT performance metrics, and the effective management of IT resources.

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

September 2023

IT Audit of the IT Governance Program

What MCIA Found

The evaluation of the County's IT governance program has identified several controls and processes that are functioning effectively to support the County's information system. Opportunities exist to further enhance the existing IT governance process and structure, by enhancing or implementing processes within the IT governance program in coordination with TEBS and departmental IT functions.

We identified nine areas of improvement to strengthen processes and mitigate risks in the following areas:

1. Implementation of risk assessment framework to evaluate the adequacy of internal controls across departmental IT functions.
2. Enhanced communication between TEBS and departmental IT functions regarding major changes to the IT management framework and IT-related systems.
3. Enhanced focus on IT-related positions and hiring process within IT functions.
4. Enhanced management of responsibility matrix between TEBS and departmental IT functions.
5. Implementation of a formalized IT strategic planning template and process.
6. Strengthening the management of innovation, quality, and technology within departmental IT functions.
7. Integration of business continuity and continuity of operations planning across departmental IT functions.
8. Enhanced tracking and review processes for assets managed by departmental IT functions.
9. Enhanced standards for IT project intake and management processes.

TABLE OF CONTENTS

Objectives

This report summarizes the information technology (IT) evaluation of Montgomery County's (the County) IT governance program (evaluation). The evaluation was performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County Office of Internal Audit (MCIA).

The evaluation included meeting with IT personnel from TEBS and selected departments[1] to obtain details around IT governance at both the County and Department/Division level. The overarching goal of this evaluation was to assess the current and planned IT governance program (structure, policies, processes, etc.).

The evaluation's objectives were:

1. Ensure IT strategies are aligned with organizational objectives.
2. Determine if IT risks are identified and managed properly.
3. Ensure IT investments are optimized to deliver value to the organization.
4. Identify the means in which IT performance is defined, measured, and reported using meaningful metrics.
5. Determine if metrics are properly implemented to provide realistic views of IT operations and governance on a tactical and strategic basis.
6. Identify whether IT resources are managed effectively.

Background

Montgomery County, Maryland is a geographically diverse county with a mix of urban, suburban, and rural areas, hosting a population of over one million residents. It spans around 500 square miles and is located in the National Capital Region, neighboring Washington, D.C. The county has a significant financial commitment, with an annual operating budget surpassing $5 billion and a capital budget exceeding $15 billion. The County places substantial investments in technology to facilitate the delivery of more than 350 services offered by its 30 functional departments and offices, employing a workforce of over 10,000 individuals.[2]

The County oversees and manages the use of hardware, software, technology, and processes through a combination of centralized and decentralized IT governance. IT governance is defined by Information Systems Audit and Control Association (ISACA) as the responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives. This approach helps the County provide high-quality services to citizens. By striking a balance between centralized oversight and department-specific implementation, the County optimizes its technological resources to achieve its goals and meet the needs of its constituents in the most effective and efficient manner.

Centralized IT Functions

[1] "Selected departments" refer to the departments evaluated during the evaluation. Due to the sensitivity of information provided by departments, and to keep departmental information anonymous, we are not attributing specific comments and information provided to a specific department.

[2] Montgomery County. (2016, June). Technology strategic plan 2016-06-01 - Montgomery County Maryland.https://www.montgomerycountymd.gov/TEBS/Resources/Files/strategic/TechnologyStrategicPlan2016-2019_Vol1.pdf

TEBS plays a vital role in providing essential IT and communication services that are critical for the smooth operation of the County's information system. These services encompass enterprise IT services and solutions, customer support, technology project management, as well as acquisitions and integrations for intricate systems. The level of support provided by TEBS to each department varies, depending on their specific requirements and the IT staff available within the department. TEBS extends its support through the following divisions, offices, and programs:

1. Office of Broadband Programs (OBP)
2. Office of the Chief Information Officer (CIO)
3. Office of Enterprise Information Security (OEIS)
4. Office of Strategy and Planning (OSAP)
5. Office of Strategic Partnerships (OSP)
6. One Face Forward (OFF)
7. Office of Change Management (OCM)
8. Office of Project Management (OPM)
9. Office of Digital Transformation (ODT)
10. Office of Public Safety Programs

TEBS is responsible for assisting County's departments with a wide range of IT and communication services to support the daily operations. These services include:

1. **Enterprise IT Services and Solutions**: TEBS offers comprehensive IT solutions and services to meet the technological needs of County departments. This includes managing and maintaining enterprise-level systems, networks, and infrastructure.
2. **Customer Support**: TEBS provides technical support and assistance to County employees and departments, helping them resolve IT-related issues and ensuring smooth functioning of their technology systems.
3. **Technology Project Management**: TEBS oversees and manages technology projects for County departments, ensuring efficient implementation, coordination, and successful delivery of IT initiatives.
4. **Acquisitions and Integrations**: TEBS handles the procurement of select assets and services and can assist in the integration of complex systems and technologies required by County departments, ensuring integration and compatibility with existing IT infrastructure.

Decentralized IT Functions

Departments within the County (with the exception of several smaller departments) are responsible for assessing and implementing advanced data, applications, teleprocessing, and radio systems either independently through internally managed IT staff or with the support and management of TEBS. The scope of the decentralized operation for departmental IT functions within the County varies depending on department's size and specific requirements of any information systems it may manage and operate.

Departmental IT functions work to address the specific needs of the department's information systems in cooperation with TEBS.

Technology Governance

Technology governance is the processes that aids in the effective and efficient use of IT resources to achieve its enterprise goals. This process involves the effective evaluation, selection, prioritization, and funding of competing IT investments; overseeing their implementation; and extraction of business benefits.

To ensure the effective management of its technology investment and plans, the County has established a multi-level technology governance structure that involves the legislative, judicial, and executive branches. Within this structure, the Office of Management and Budget (OMB) and TEBS work together to review IT budget requests submitted by departments. Funding for departmental technology staff, contractors, and specific projects may be contained in separate departmental budgets managed and approved by OMB. This collaborative process allows for the rating and assessment of IT projects, determining their priority, and allocating resources based on established criteria.

TEBS is currently in the process of enhancing the centralized IT governance model through the implementation of a three-phase plan.

Phase One: This phase involves the revision and communicating of the Administrative Procedure 6-1: Acceptable Use of County Technology Policy. The implementation of the revised AP 6-1 policy requires TEBS review and approval of all departmental requests for new network equipment, network/broadband services, applications, and cloud services that connect to the County's network. Included in this stage is also the initial iteration of the Service Catalog. The implementation of the Service Catalog will help clarify specific enterprise services TEBS offers to departments and offer a centralized intake for service requests.

Per discussion with TEBS leadership, Phase One has since been implemented post completion of this assessment.

Phase Two: In this phase, TEBS will introduce the second iteration of the Service Catalog. The second iteration of the Service Catalog will mainly consist of the implementation of the ServiceNow system as a backend to the SharePoint site. The integration of ServiceNow with the Service Catalog will facilitate and improve the efficiency, management, and quality of service that TEBS can provide to departmental IT functions.

Per discussion with TEBS leadership, Phase Two has since been implemented post completion of this assessment.

Phase Three: The final phase is dedicated to stabilizing the implemented changes, enhancing project management capabilities, and evaluating the progress made in phases one and two. To do this, the County Executive has asked TEBS to establish a Chief Information Officer (CIO) reporting relationship that formalizes the relationship between the departmental IT leads in some of the largest County departments with the Enterprise CIO to align technology goals with process maturity.

Scope and Methodology

The evaluation was conducted from October 2022 to April 2023. The evaluation focused on the following:

1. Overall strategic approach to implementation and effectiveness of IT Governance processes and subprocesses throughout the County.
2. Ensuring the County's IT strategies are aligned with organizational objectives.
3. Confirming that IT risks are identified and managed properly.
4. Determining whether there are documented short- and long-term goals and initiatives that focus on enhancing the IT environment based on entity-wide objectives.
5. Verifying that goals and initiatives are reviewed and authorized by management, tracked for progress, and periodically evaluated for necessary updates.

6. Verifying the existence of an IT Steering Committee or similar council that is comprised of key IT personnel, and is responsible for the overall IT environment and strategic objectives.
7. Determining whether critical IT policies and procedures have been developed and are properly maintained and clearly communicated.
8. Verifying that critical system users are aware of, and document their adherence to, the County's information security guidelines.
9. Determining whether the County measures and improves itself based on industry trends and practices adopted by peers.
10. Determine whether activity is monitored for compliance with laws, regulations, rules, and industry standards, and modifications are made to include regulatory change.

SC&H adopted a two-phased approach to evaluate the objectives outlined above. In phase one, a survey assessment was conducted, followed by phase two, which involved conducting interviews with select departmental IT functions.

Phase I: Surveys

SC&H issued surveys to 60 identified lead IT individuals across 36 departments and divisions focused on understanding and evaluating the current state of IT governance and oversight. Results were received from 24 individuals across 20 departments and divisions. The survey included questions related to, but not limited to, the following (Refer to **Appendix: A** for details):

1. Alignment of IT strategies with organizational objectives
2. IT risk identification and management
3. IT investment procedures and communication
4. Processes to define, measure, and report IT performance
5. Implementation of metrics to for IT operations and governance on a tactical and strategic basis
6. IT resource management

Based on the results of the survey, SC&H identified common themes of risks and concerns across the various departments and divisions, providing insights into the current state of IT governance in the County (Refer to **Appendix: B** for additional details). To ensure accuracy and clarity, SC&H conducted follow-up inquiries as necessary to clarify initial responses. Once these clarifications were obtained, SC&H proceeded to analyze the results to identify areas for targeted, in-depth interviews.

This approach allowed SC&H to gain a comprehensive understanding of the specific risks and challenges faced by each department and division, enabling us to delve deeper into those areas during the subsequent interview phase. By conducting these targeted interviews, SC&H aimed to gather more detailed information and insights to further evaluate the state of IT governance within the County.

Phase II: Interviews

Based on review of survey responses and recommendations from MCIA, targeted assessments were conducted through interviews and walkthroughs across nine departments and divisions. These departments included:

1. Technology and Enterprise Business Solutions (TEBS)
2. Office of Human Resources (OHR)
3. Finance (FIN)
4. Alcohol Beverage Service (ABS)
5. Health and Human Services (HHS)

6. Fire and Rescue Services (FRS)
7. Office of Emergency Management (OEMHS)
8. Transportation (DOT)
9. Police (POL)

The primary objectives of these interviews were to:

1. Further understand and confirm IT governance processes identified in the survey responses.
2. Obtain and/or observe evidence that substantiated survey responses.
3. Identify the current state of processes and procedures related to IT governance at the County, Department, and Division level.
4. Identify IT governance risks based on interview results.

In order to achieve the objective of evaluating the enterprise governance of information and technology at Montgomery County effectively, SC&H primarily relied on the framework provided by ISACA's Control Objectives for Information and Related Technologies (COBIT) 2019 Volume 1.1. COBIT is a widely recognized framework globally, designed to govern and manage enterprise information and technology (I&T). Additionally, SC&H incorporated supplementary controls to address specific objectives and concerns that were identified during the Phase I stage of the assessment. This approach ensured a comprehensive evaluation of the organization's governance and management practices in the field of information and technology.

During the interview phase, an assessment was conducted on enterprise and department-level IT-related policies, procedures, and processes. The evaluation focused on six key domain areas, which are as follows:

1. Tactical alignment
2. Stability and reliability
3. Processes and standards
4. Technology leverage/support
5. Managing IT operations
6. Results management and human capital

SC&H documented conclusions, including risks and recommendations, for applicable controls within the six key domain areas referenced above. These conclusions were derived from analyzing responses received during the interviews, as well as evaluating relevant supporting documents. SC&H identified potential risks associated with the current state of IT governance throughout the County. These identified risks and corresponding recommendations highlight areas that require additional attention and opportunities for continued growth in policy and procedure to enhance and mature MCG’s overall IT governance practices.

Please refer to the table below for more details about the domains and control descriptions assessed throughout the evaluation.

Domain	Control	Control Description
TA - Tactical Alignment	Managed IT Management Framework	A consistent management approach for enterprise governance is implemented including components such as management processes; organizational structures; roles and responsibilities; reliable and repeatable activities; information items; policies and procedures; skills and competencies; culture and behavior; and services, infrastructure and applications.
	Managed Strategy	Digital transformation strategy of the organization is being conducted. A holistic IT approach, ensuring that each initiative is clearly connected to an overarching strategy, enables change in all different aspects of the organization, from channels and processes to data, culture, skills, operating model and incentives.
	Managed Innovation	Appropriate parties, including TEBS and Departments and Divisions in charge of IT processes, achieve competitive advantage, business innovation, improved customer experience, and improved operational effectiveness and efficiency by exploiting IT developments and emerging technologies.
	Managed Portfolio	Appropriate parties optimize the performance of the overall portfolio of programs in response to individual program, product and service performance and changing enterprise priorities and demand.
	Continuous Monitoring of Managed Portfolio	Continuous monitoring of the performance of the overall portfolio of programs, product and services, and changing enterprise priorities are executed periodically.
	Managed Service Agreements	IT products, services and service levels are reviewed periodically to ensure they meet current and future enterprise needs.
	Managed Quality	Consistent delivery of technology solutions and services occurs to meet the quality requirements of the enterprise and satisfy stakeholder needs.
SR - Stability and Reliability	Ensured Governance Framework Setting and Maintenance	Enterprise's strategies, objectives, and desired value, related to IT initiatives are transparent to MCG stakeholders; compliant with legal, contractual and regulatory requirements; and the governance requirements are met.
	Managed Availability and Capacity	Continuous service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements is executed.
	Ensured Resource Optimization	Resource needs of the County are met in the optimal manner necessary to support IT functions throughout the County.

Domain	Control	Control Description
	Managed Continuity	Continuously adapt business operations and maintain availability of information technology resources and data at a level acceptable to the County, Department, and Division in the event of a significant disruption (e.g., threats, opportunities, demands).
PS - Processes and Standards	Managed Programs	IT Programs throughout the County manage and track desired business values and the reduction of unexpected delays, costs and value erosion through communications and collaboration with IT and end users.
	Managed IT Changes	Fast and reliable delivery of changes to information systems is executed while reducing the risk of negatively impacting the stability or integrity of the changed environment.
	Managed Assets	IT assets are tracked and accounted for throughout their life cycle.
	Managed Projects	IT project outcomes are defined to reduce the risk of unexpected delays, costs and value erosion through communications and involvement of business and end users with IT.
TL - Technology Leverage/Support	Managed Operations	Deliver IT operational product and service outcomes as planned.
	Managed Service Requests and Incidents	Increase productivity and minimize disruptions through timely resolution of user queries and incidents.
	Managed Business Process Controls	Maintain information integrity and the security of information assets handled within business processes in the enterprise or its outsourced operation.
	Technology Leverage	Technology is used to optimize operations, create efficiencies and maximize revenue.
RM - Results Management	Managed Performance and Conformance Monitoring	Provide transparency of performance and conformance and drive achievement of goals.
	Managed System of Internal Control	Provide transparency for key stakeholders on the adequacy of the system of internal controls to improve trust in operations, confidence in the achievement of enterprise objectives, and an adequate understanding of residual risk.
	Managed Compliance With External Requirements	IT operations executes initiatives that are in compliance with all applicable external requirements.
HC - Human Capital	Managed Human Resources	Optimize human resources capabilities to meet enterprise objectives.

Domain	Control	Control Description
	Managed Relationships	Establish and document effective use of resources discussions between TEBS, Departments, and Divisions to ensure knowledge, skills and behaviors are communicated to create improved outcomes, increased confidence, mutual trust and effectiveness to stimulate a productive relationship across IT resources within the County.
	Ensured Stakeholder Engagement	Stakeholder engagement is solicited to support the IT strategy and road map, identify areas of improvement, and confirm that IT related objectives are in alignment with the County's strategy.

Summary of Work

Based on the performed audit evaluation procedures, we have identified nine risks associated with IT governance within the County. These risks have been identified based on common themes observed during the survey and fieldwork interview evaluation phase. Detailed testing procedures were not conducted to establish comfort over implementation and operating effectiveness of controls. Findings/observations are based on survey and interview results. Additionally, for each identified risk, we have provided possible recommendations aimed at operational improvements and risk mitigation activities.

During the evaluation, it was observed that the majority of IT operations under the existing governance framework are operating as intended. Furthermore, there are plans in place for continuous improvement, aiming to enhance IT performance and achieve better outcomes. This proactive approach to continuous improvement demonstrates the commitment to optimizing IT operations and delivering improved results. Based on the current state of centralized IT oversight and department-specific implementation, there are predictable tensions that may be created as an organization attempts to develop and mature controls and processes that support an enhanced IT governance model.

We extend our appreciation to the management and staff of TEBS and departmental IT functions that participated in this evaluation for their assistance and cooperation. Should you have any questions or comments regarding the information presented in the IT Governance report, please feel free to reach out to us.

Risks and Recommendations

The following nine risk and recommendations represent a collection of observations identified during the review and may not apply to every department reviewed in this audit. These findings serve to promote a culture of continuous improvement and encourage the adoption of best practices to enhance IT performance and outcomes.

As previously noted, it is not the intent of this review to identify specific concerns and individual issues attributable to a specific department. Rather, the intent of the review is to identify opportunities for improvement within the County’s current IT governance model that could help optimize IT operations across the County.

Risk Level - Risk Description and Necessary Actions

The characterization of “risk” speaks to our assessment of the time-sensitivity and potential impact of the County’s taking (or not-taking) appropriate actions to address the findings identified during the audit: higher risk = greater time sensitivity to take “corrective” actions as soon as possible, and the potential impact to the County’s successful implementation of a robust IT governance model.

High - There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan should be put in place as soon as possible.

Medium - Corrective actions are needed and a plan should be developed to incorporate these actions within a reasonable period of time.

Low - The system’s owner must determine whether corrective actions are still required or decide to accept the risk.

Tier 1 – High Risk

Risk and Recommendation #1

Risk #1:
Ensuring there are appropriate control and processes in place for IT systems is an important component to identifying vulnerabilities and gaps in the information system that could potentially lead to significant damage risk to operations and data exposures.

Based on procedures performed, we identified a lack of formal process throughout the County to assess and measure the adequacy of internal control systems of departmental IT functions. While most departments are aware of enterprise IT-related policy and procedure documents (AP series policy and procedure documents), there is no established process to review the proper implementation of these enterprise IT guidelines.

We noted that TEBS is in the process of building a risk assessment team that will perform risk assessment on enterprise and departmental systems and report to the CISO’s office.

Recommendation #1:
We recommend the design and implementation of an IT security risk assessment process to require periodic completion of a formal documented risk assessment of critical systems that are managed by departmental IT functions. This will increase transparency for key stakeholders regarding the effectiveness of internal controls, enhance trust in operations, confidence in achieving enterprise objectives, and enable a better understanding of residual risks. Consideration should include an independent review and examination of an IT systems policies, records and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

The risk assessment should be periodically performed in collaboration with system owners from departmental IT functions and internal or external IT auditors. IT security auditors can be CISO personnel, county internal auditors, private auditing firms, or augmented staff from existing internal audit teams that have the experience and expertise required to perform IT security audits. The IT security audit plan should be established using industry-standard security controls to assess confidentiality, integrity, and availability. A report should be issued and

decimated to appropriate personnel within the County after the assessment, including all findings.

Risk and Recommendation #2

Risk #2:
Preemptive communication – from the initial planning period of major IT changes to the IT management framework and IT related systems, prior to approval and scheduled implementation – can impact the success of both countywide and department-specific IT functions and business operations.

At the time of the evaluation, major IT changes impacting the County's IT management framework were primarily communicated via a periodic Technology Operations Management Group (TOMG) briefing meeting. Departments expressed a perception that this forum was primarily used to inform departmental IT functions about upcoming or already implemented IT-related policy or system changes, rather than a forum designed for departments and TEBS to collaborate on major IT policies and changes. It should be acknowledged that certain policies and changes are appropriately "top-down" in nature, and in such cases, there is a heightened importance to articulate the basis for such policies and changes and to discuss potential impacts on departments.

Therefore, it is necessary to ensure there is a formal and collaborative process that engages departmental IT functions during planning and decision-making processes of major changes. This can facilitate the identification and resolution of any risks and concerns raised by departmental IT functions before (whenever possible) a major policy or system-related change is implemented, thereby minimizing the impact on the county's information systems, and ensuring uninterrupted business operations.

Recommendation #2:
To foster a collaborative environment for departmental IT functions and for major IT decisions to consider the unique information system environments across departments, we recommend assessing the current TOMG process for formally engaging departmental IT functions during decision-making and planning processes for major IT changes that may have a significant impact on the County's information systems. This formal process should be a forum for discussion to understand and answer departmental IT functions questions and concerns. It should not be an impediment for innovation and change within the County.

This formal engagement could take the form of scheduled periodic meetings, such as the TOMG, involving all IT leads throughout the County. The agenda of these meetings would be to provide briefings on upcoming major IT changes under consideration. During these sessions, TEBS might announce proposed IT-related changes. Departmental IT functions would be presented the opportunity to voice potential suggestions or concerns based on their knowledge of the information systems they manage.

This collaborative process will identify and address any risks or concerns raised by departmental IT functions prior to implementing significant policy or system-related changes to the county's information systems. By involving all departments, this approach will promote transparency and ensures that departments are aware of upcoming changes, allowing them to prepare their information systems accordingly in advance.

The goal is to foster effective communication, proactive planning, and alignment among departments to minimize disruptions and optimize the implementation of IT changes within the county's information systems.

Risk and Recommendation #3

Risk #3:
Ensuring sufficient human capital in the County's IT functions can promote improved efficiency, and reduce the risk of security breaches, downtime, decreased innovation, and employee burnout.

At the time of the evaluation, we noted that the classification specifications and job descriptions for IT-related positions throughout the County were not regularly updated, reviewed, and maintained. Job descriptions serve as the foundation for the work that employees should expect to perform on a daily basis and give managers a road map for performance evaluations. When aligned with a strategy, the classification specifications and job descriptions become vitally important in recruitment, retention, skill-building and career development.

Recommendation #3:
We recommend the County undertake a review of IT-related classification specifications and job descriptions to ensure they align with the current industry standards and requirements in the fast-evolving information technology landscape. By ensuring that the classification specifications and job descriptions accurately reflect the skills and qualifications needed in the IT field, the organization could attract and retain top talent, help effectively meet the challenges of the technology landscape, and more easily adapt to emerging trends and technologies. This proactive step could support the organization in building a skilled and capable IT workforce.

We also recommend the County review and update the career and application site with current industry-standard models to modernize and improve applicants' experience during the hiring process. By utilizing the latest industry-standard HR solution models and automation, the hiring process can be streamlined for both the hirer and the applicant.

These efforts will require a collaborative process involving the County's Office of Human Resources, TEBS, and other stakeholders.

Tier 2 – Moderate Risk

Risk and Recommendation #4

Risk #4:
It is important, particularly during any period of changing IT roles and responsibilities that there be a defined and maintained responsibility matrix between TEBS and departmental IT functions can lead to confusion, inefficiencies, and gaps in responsibilities, potentially resulting in a lack of accountability and suboptimal IT performance.

Recommendation #4:
SC&H noted that TEBS has implemented an updated service catalog as a SharePoint front end site as part of the Phase one IT centralization and IT governance initiative. The service catalog should include comprehensive metrics that clearly outline the service capabilities and responsibilities of both TEBS and departmental IT functions. Additionally, TEBS should actively

seek feedback from departments to further improve the functionality of the service catalog and the overall service provided. By incorporating these recommendations, TEBS can enhance the effectiveness and usability of the service catalog, aligning it more closely with the needs and expectations of the departments it serves.

Risk and Recommendation #5

Risk #5:
Ensuring that there is an integrated and formal IT strategic planning process is critical to effectively aligning IT strategy with business strategies and to ensure that relevant internal and external trends that may impact the County are factored into the planning process.

Our observations indicate that most departmental IT functions do not have a formally documented, periodically reviewed, and updated IT strategic plan in place. Our review did not identify any requirements at the County level that require departments to document departmental IT strategic plans. Nor could we identify any resources, tools, or processes reflecting best practices that have been shared with departments to facilitate or promote such planning.

Recommendation #5:
To consistently implement and to further enhance the alignment between departmental IT function plan and the enterprise-managed strategic plan, it is recommended that the County implement a formalized IT strategic plan template that can be customized and regularly updated by the departmental IT function. By doing so, departmental IT functions can tailor their plans to their specific needs while remaining aligned with the overarching strategic plan of the organization.

A formalized IT strategic plan will enable departmental IT function to clearly establish their goals and objectives and provide a benchmark for monitoring conformance and performance of the information systems they maintain. It will also help identify gaps and areas for improvement, enabling departmental IT function to develop strategies and tactics to address them.

To create an effective IT strategic plan, the template should include the following key components; vision and mission statement, SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, goals and objectives, IT initiative and projects, risk management, budget and resource allocation, performance metrics, and implementation roadmap. Overall, an IT strategic plan should be a comprehensive document that aligns the IT department's goals and objectives with the organization's overall business strategy. It should provide a clear roadmap for achieving success and provide a framework for ongoing governance and management of IT resources.

Risk and Recommendation #6

Risk #6:
Our review did not identify a formal or consistent process for the County (and the departments) to assess emerging technologies and the adequacy of (and projected longevity of) existing technology/systems. The absence of a regular assessment process could lead to suboptimal operations and inefficiencies in County operations and systems.

Our observations indicate an inconsistent approach to managed innovation, quality, and technology leverage within the departmental IT functions. This may be attributed to the

departments having a lower appetite for change, and the absence of a process to review existing technology with new and current industry-standard alternatives.

Recommendation #6:
We recommend the County consider implementing a periodic assessment process, potentially as a component of the strategic planning process discussed above, that would facilitate a comprehensive evaluation of existing systems to identify any legacy systems that are outdated or ineffective. Based on this evaluation, the County/departments should prioritize systems that require immediate replacement and develop a corresponding migration plan.

As part of the IT Strategic Plan, it is essential for departmental IT function to assess their current systems and develop a clear strategy for prioritizing and replacing legacy technology (websites and application system) with modern and efficient technology solutions. By doing so, departmental IT function can enhance productivity and improve the overall quality of services provided to customers.

Risk and Recommendation #7

Risk #7:
It is critical to sufficiently integrate and align business continuity planning (BCP) and continuity of operations planning (COOP) processes. Ensuring formal documentation and periodic review of BCPs can as part of COOP planning can minimize the risk to the County's business operations and information system availability in case of any disruption.

The maintenance of BCPs across departmental IT functions throughout the county is inconsistently managed and enforced. We noted that certain departments maintain well-maintained and regularly updated BCPs, however, others do not document or review such plans in a consistent and/or formal manner.

Recommendation #7:
We recommend that TEBS and the County's Office of Emergency Management and Homeland Security (OEMHS) collaborate to ensure there is an integrated BCP/COOP policy and management process across County departments and offices to ensure that critical business operations can continue operating during and after disruptive events, such as natural and human-induced disasters and cyberattacks, and that there are appropriate recovery strategies to restore critical functions, including roles and responsibilities, communication plans, and test scenarios.

Such an integrated process should help ensure that regular training and testing is conducted in accordance with County policy to ensure the plan's effectiveness. It's also essential to conduct periodic reviews and updates of the plan and make necessary changes based on lessons learned from these tests and drills.

Tier 3 – Low Risk

Risk and Recommendation #8

Risk #8:
Inconsistent tracking of IT assets and reporting of the assets throughout the County, can lead to an increase in security risks, wasted resources, and issues in asset lifecycle management.

TEBS currently manages major IT assets throughout the county using the DCM (Device Client Management) system. However, there is additional unmitigated risk associated with IT assets obtained and managed directly by departmental IT functions.

Our review procedures indicate that there is inconsistency in the documentation, tracking, and review of IT assets owned and managed by the departmental IT functions. This is due to the lack of a formal asset management procedure for assets owned and managed by departmental IT functions. These devices should be accounted for and properly managed to ensure their security, functionality, and alignment with organizational objectives.

Recommendation #8:
We recommend that TEBS formulate a standard policy and procedure for IT asset management to ensure consistent management of all IT assets owned and managed by departmental IT functions. The standard asset management procedure document should include a requirement for departmental IT functions to maintain documented inventory of assets, including relevant information such as asset component description, version, location, owner, and supporting documentation.[3]

Risk and Recommendation #9

Risk #9:
Effective management of IT projects/enhancements is critical to the successful implementation and deployment of new systems or enhancement to existing systems. The absence of a standard for IT project management may lead to unauthorized project initiation and unfulfilled requirements, potentially resulting in wasted resources, delays, and increased costs.

Recommendation #9:
SC&H noted that TEBS is in the process of implementing processes which will serve as a standard for managing IT projects.

We recommend that implementation of IT Project Management procedures includes detailed requirements for IT, business, and end-users regarding the management of IT projects. Additionally, it should require departmental IT functions to notify TEBS before starting new IT projects, ensuring that TEBS has visibility and oversight into all IT projects throughout the County.

[3] As part of phase one TEBS IT governance improvement plan, TEBS is currently revising the AP 6-1 policy document. This revision aims to reinforce the requirement that departments must not purchase or connect any device or application to the county networks without sufficient authorization from TEBS. Additionally, it emphasizes that departments should not establish new network connections without obtaining proper authorization from TEBS. These measures are essential to ensure proper control and security of the county's IT infrastructure and networks, addressing the risk identified in Finding 6.

Comments and MCIA Evaluation

We provided the Office of Human Resources (OHR), the Office of Emergency Management and Homeland Security (OEMHS), and the Technology and Enterprise Business Solutions (TEBS) with a draft of this report for review and comment. Their responses are summarized below.

OEMHS responded that it did not have any formal comments, but agreed with the recommendation to synergize the business continuity planning and continuity of operations planning processes with TEBS, and looked forward to doing so.

OHR, while not disagreeing with the report findings and recommendations, noted that the County "does not have in-house expertise and staffing to conduct and produce a study of "all IT-related classes"." OHR indicated that there are more than 21 IT related classes of work, over 229 incumbered IT related positions, working in more than 25 departments. A study of this size "would need to consider all the work to assure positions are stratified and assigned in the ways we deliver IT functions." OHR advised further that "an outside resource and sufficient funding to deliver a study of this magnitude", along with the commitment of all parties for this work.

TEBS responded, agreeing with eight of the nine recommendations, and discussing progress TEBS had made in implementing enhancements to existing policies and processes, including those to implement direction from the Chief Administrative Officer's November 23, 2022, memorandum, "*Updating our Information Technology Governance Model*." TEBS disagreed with Recommendation #2, that the County assess "the current TOMG process for formally engaging departmental IT functions during decision-making and planning processes for major IT changes that may have a significant impact on the County's information systems." TEBS notes several current forums – including the Technical Operations Management Group (TOMG), the Senior Management Team, and the quarterly cybersecurity briefings with selected staff and County government offices as mechanisms that address the risks identified during the review and discussed in the report. MCIA did not believe a change in the report's findings and recommendations is warranted based on TEBS response; we believe the County should continue to assess whether the existing forums are sufficient to provide a "formal and collaborative process that engages departmental IT functions during planning and decision-making processes of major changes."

The TEBS response is incorporated in the report at Appendix A.

Appendix A – Department Comments

DEPARTMENT OF TECHNOLOGY AND ENTERPRISE BUSINESS SOLUTIONS

Marc Elrich
County Executive

Gail M. Roper
Chief Information Officer/Director

MEMORANDUM

August 24, 2023

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

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

SUBJECT: Formal Comments on Draft Report: "Information Technology Governance Evaluation" – July 2023

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 Danni Melton-Russell or myself.

cc: Shayna Taqi, Change Management Division Chief, TEBS
Ivan Galic, Division Chief, One Face Forward Initiative, TEBS
Keith Young, Chief Information Security Officer, TEBS
Keisha Lewis, Project Management Division Chief, TEBS
Alison Dollar, Chief Budget Officer, TEBS
Danni Melton-Russell, 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.

On November 23, 2022, the Chief Administrative Officer (CAO) issued a memo titled: "Updating our Information Technology Governance Model." This memo directed TEBS to implement an enterprise driven IT governance model and to work towards a more innovative, collaborative, centralized, cost-efficient, secure, and resilient IT function across the County government. In this effort to accomplish the CAO's goal of eliminating duplication of services and assets in local departments by centralizing enterprise functions within TEBS, the Office of Human Resources (OHR) IT staff were consolidated into TEBS. Going forward, TEBS will support OHR and the Employee Retirement System (ERS).

In response to the CAOs directive, a cross-functional workgroup was formed within TEBS to identify opportunities for improvements to Montgomery County's federated IT Governance model. From Fall 2022-Spring 2023 the group accomplished the following:

- Identified various areas for improvement, established strategic goals and developed a tactical plan to incrementally address policy and process improvements.
- Enhanced the service delivery by publishing a Service Catalog, thereby creating a central place for service request intake and implementing a new system to track service requests and enable service level agreement (SLA) standards. Developed a process to deliver prompt response times, thorough review of service requests and proper assignment of resources. Note that the Service Catalog supplements the IT support services provided by the Enterprise IT Help Desk.
- Improved security through increased oversight of IT configuration and acquisition. In support of the updated Administrative Procedure 6-1, TEBS developed a process for departments to obtain prior approval to purchase/connect any device, application, or network connection to the County network. These process improvements and policy revisions were communicated to and vetted with many departments, Technical Operations Management Group (TOMG)/IT Contacts and TEBS staff.

Starting March 2023, TEBS began evaluating remaining disparate intake processes to integrate into the centralized Service Catalog intake process. Each process refinement is being prioritized

into the iterative project plan and will include collaboration across TEBS divisions and the functional business owners. Additional process enhancements slated for the next phase of work include implementing the newly standardized project management process and project intake and continuing to improve the Service Catalog.

This work represents a continuous improvement effort with iterative phases in which TEBS will: identify process or policy changes needed to enhance the IT Governance model, prioritize work efforts, develop implementation plans, engage business owners and user communities, communicate and implement changes, evaluate changes and make additional policy/process revisions as needed, and repeat.

Recommendation #1: Implementation of risk assessment framework to evaluate the adequacy of internal controls across departmental IT functions.

TEBS Response:
TEBS concurs with this recommendation and as noted in the report, TEBS is already in the process of hiring and building a risk assessment team that will report to the Chief Information Security Official (CISO) and will perform risk assessments on enterprise and departmental systems.

Recommendation #2: Enhanced communication between TEBS and departmental IT functions regarding major changes to the IT management framework and IT-related systems.

TEBS Response:
TEBS cannot concur with the risk nor the recommendation. TEBS requested examples of IT risk that resulted from changes to the IT Governance framework and were not provided any as it would violate the confidence promised to the interviewees. This in conjunction with the lack of any demonstrated outages or other significant IT events (that were brought to TEBS awareness as related to IT governance changes), TEBS cannot concur with the finding nor its identification as high risk.

There are several formal and informal communication institutions that currently exist and were in effect in the review period that the review did not consider. The Technical Operations Management Group (TOMG) is a formal mechanism to communicate changes, get IT staff feedback on upcoming changes, and identify risks at the staff level. TEBS provides a comment

period on all enterprise IT policy changes to the TOMG group. TEBS regularly presents TOMG members the opportunity to participate in pilot projects and test groups so they can identify risks and unintended outcomes from enterprise changes. The Senior Management Team (SMT) meetings are also a formal mechanism for Department Directors to provide departmental feedback to TEBS/CEX on decisions and impending IT changes. Additionally, there is a quarterly cybersecurity briefing with selected staff from TEBS, County Council, CAO, DCAO, the Department of Finance (FIN), and the Office of County Attorney where risks and upcoming security improvements are planned and discussed. These meetings are focused on protecting the enterprise from escalating cyber threats. All of these practices have been in place for over 2 years and thus TEBS cannot concur with the recommendation as it has already been implemented.

In addition to these regular communication institutions, TEBS in conjunction with FIN and MCIA completed the Business Impact Analysis to better understand departmental systems and their dependencies, their recovery time objectives, and recovery point objectives. Beyond that initial study, conversations with relevant officials in departments and senior leadership have continued informally about the enterprise and departmental efforts to improve cybersecurity and resiliency of our systems. TEBS continues to use ad-hoc and agile meetings on the most relevant topics to convene departments which is a best practice as opposed to standing meetings with static attendees which provide less value.

Recommendation #3: Enhanced focus on IT-related positions and hiring process within IT functions.

TEBS Response:
TEBS agrees with the finding that "job descriptions for IT-related positions throughout the County were not regularly updated, reviewed, and maintained" and looks forward to continuing to work collaboratively with OHR in their process to update the position descriptions. In addition, TEBS is taking a comprehensive approach to ensuring the IT position job classes and position descriptions are best able to support the IT governance structure of the future. This includes abolishing certain vacant IT positions, creating entirely new IT job classes such as the recently created IT Project Manager positions, and reviewing all new department IT positions requests submitted to OMB.

Recommendation #4: Enhanced management of responsibility matrix between TEBS and departmental IT functions.

TEBS Response:
TEBS concurs with this recommendation. Implementation of this recommendation is complete. In May 2023, TEBS deployed the second version of the internal Service Catalog utilizing the ServiceNow platform. This service catalog clearly outlines the service capabilities of TEBS that are available to departments, the request process, and the service level agreement (SLA) for TEBS response. TEBS has received feedback from department users and is working through a backlog of those improvements and integrations as part of an ongoing continual improvement process.

Recommendation #5: Implementation of a formalized IT strategic planning template and process.

TEBS Response:
TEBS agrees with this finding and acknowledges the need to better engage departments in IT strategic planning. However, TEBS disagrees that this recommendation should be targeted at the department level as this is inconsistent with the vision for consolidation of IT. TEBS is best able to engage and lead strategic planning at an Enterprise level, while also planning for department engagement in those efforts. For example, a Cloud-first strategy, Business Continuity initiative, Business Impact Analysis efforts, and leveraging of Artificial Intelligence (AI) to solve County problems, are best defined and implemented at the Enterprise level. A centralized strategy is best suited for Montgomery County as opposed to the review's recommendation of facilitating departments having their own strategies which may or may not align with the County's Enterprise strategy and Enterprise investments. TEBS has completed a draft of an Enterprise IT Strategy document with direction from the CIO and with inputs across each Division. To finalize this document, TEBS will engage departments to ensure alignment between department needs and TEBS efforts to meet County goals.

Recommendation #6: Strengthening the management of innovation, quality, and technology within departmental IT functions.

TEBS Response:
TEBS concurs with the finding and will take an enterprise approach as opposed to a departmental approach by prioritizing the replacement of multiple legacy systems at one time by selecting enterprise offerings. For example, TEBS is working thorough a collaborative discovery effort to replace the legacy Customer Relationship Management (CRM) system with a new enterprise offering. Additionally, by building the asset and application inventory (referred to

below in response 8) TEBS and departments will have a greater view into legacy applications and be able to plan and replace systems before they reach end of vendor support.

Recommendation #7: Integration of business continuity and continuity of operations planning across departmental IT functions.

TEBS Response:
TEBS concurs with this recommendation and will work with your office to implement the recommendation in conjunction with the Office of Emergency Management and Homeland Security (OEMHS).

Recommendation #8: Enhanced tracking and review processes for assets managed by departmental IT functions.

TEBS Response:
Related to Finding 8 TEBS agrees with the finding. The County's Information Security Policy (AP 6-7) applies to all IT assets purchased by the County, both at the enterprise and departmental level and has requirements related to asset disposal and identification of owners. TEBS currently has an asset database and scans all County assets at least weekly for inventory and security vulnerabilities, but that information is not in a central repository and not all departmental IT staff have access. TEBS plans to submit a budget request in FY25 to have resources for county-wide management of assets on the County network. Additionally, TEBS has implemented a Network review board to reinforce the AP 6-1 requirement that departments must not purchase or connect any new devices, hardware, cloud services, or applications to the County networks without sufficient authorization from TEBS.

Recommendation #9: Enhanced standards for IT project intake and management processes.

TEBS Response:
TEBS concurs with this recommendation and as noted in the report, TEBS is in the process of implementing processes which will serve as a standard for managing Enterprise-level IT projects. Enterprise-level projects will also undergo periodic phase-gate reviews by a project review board. Project Review and Project Management have been added to the Internal IT Service Catalog and can be requested by departments at any time.

TEBS appreciates this opportunity to provide formal response.

Appendix B – Survey Questionnaire

#	Question
1	Please select your department
2	Within your department, who is responsible for managing IT Governance? (Please list all that apply)
3	What Executive Leadership team do you report to?
4	What is the frequency of communication with the Executive Leadership team identified in the above question? [Please select all that apply]
5	What are the methods used to communicate with the Executive Leadership team identified above? [Please select all that apply]
6	Does your Department have a formal Departmental IT Strategic Plan?
7	How far out does your IT Strategic Plan span?
8	Is your Department/Division involved in Enterprise IT strategic planning?
9	Please describe your Department's involvement in Enterprise IT strategic planning.
10	How are IT projects chosen for review? [Please select all that apply]
11	Is the approval process for IT projects formal and consistent across all types of project requests?
12	Please describe if IT projects require more than a single review (e.g., concept, full proposal, milestones)?
13	Indicate whether the IT project review process evaluates....[Please select all that apply]
14	What global and/or industry-level IT frameworks/standards are followed or leveraged by your Department [Please select all that apply]
15	What types and frequencies of metrics and reporting are in place specific to the status and health of the department's function?
16	How does your department measure IT performance for people, service, and technology (e.g., periodic feedback from users, etc.)?
17	Does your department have processes in place to manage the handling of PII and/or other sensitive data
18	Have departmental IT risk tolerances been established?
19	What would you consider strengths within the current model of IT governance?
20	What weaknesses and/or areas of improvement exist within the department's current model of IT governance?
21	What are the main barriers/challenges to developing/maintaining IT governance? [Please select all that apply]